HACKER JOURNAL

Anno 2 - N. 17
16 Gennaio/30 Gennaio 2002

Boss: theguilty@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Karin Harrop

Contributors: aDm, Bismark.it, Enzo Borri, CAT4R4TTA, Roberto "decOder" Enea, Khamul, Lele-Altos.tk, {RoSwEiL}, Paola Tigrino

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

LAMPADINE SOTTO COPYRIGHT

Se di recente siete stati a Parigi e pensate di di pubblicare su un sito Web le foto che avete scattato, dovete fare un po' di attenzione. Se tra le immagini scattate di notte ne trovate qualcuna della torre Eiffel illuminata, sappiate che non avete il diritto di pubblicarla. La SNTE, la società che ha realizzato l'illuminazione della torre, possiede infatti i diritti di sfruttamento dell'immagine della sua opera. Poco importa che la torre sia il simbolo di Parigi, che sia di dominio pubblico non solo dei francesi ma dell'Umanità intera, o che il signor Eiffel abbia rinunciato ai diritti sull'immagine subito dopo l'inaugurazione. Se volete pubblicare un foto "notturna" della più celebre torre d'acciaio al mondo, dovete pagare.

E lo stesso potrebbe capitarvi se scattate la foto di una casa, un palazzo, una statua, un affresco. Con il lodevole intento di tutelare la privacy e il diritto alla tutela della propria immagine e di quella delle proprie produzioni, la legge francese sul copyright ha finito col concedere ai cittadini e alle aziende un potere immenso. E non mancano gli eccessi e i paradossi.



Così capita che un tale faccia causa al fotografo che ha realizzato una cartolina col lungomare di una località balneare, perché sulla strada sta passando la sua moto (senza che tra l'altro si riesca a leggerne la targa). O che una coppia citi in giudizio l'Ente del Turismo perché, su un depliant promozionale, una foto aerea ritrae la loro villetta.

Tempo fa, queste limitazioni sarebbero state tutto sommato piuttosto leggere: solo chi intendeva sfruttare commercialmente le foto avrebbe dovuto prendere accordi col proprietario dei diritti all'immagine (quindi solo gli editori di giornali, cataloghi, libri di fotografie, pubblicità...). Ora che chiunque può pubblicare le proprie foto sul Web con pochi clic, senza chiedere soldi a chi visita il sito, questa legge appare quanto meno esagerata.

grand@hackerjournal.it

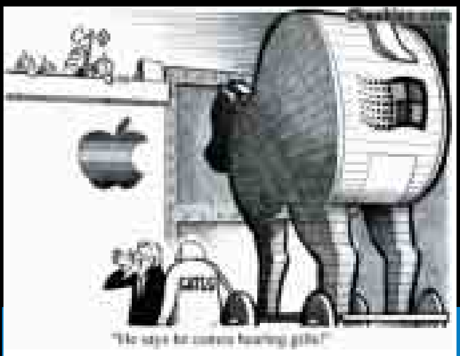
mailto:
redazione@hackerjournal.it

LE MERAVIGLIE DEL P2P

Ho appena letto il vostro articolo "pagare per il P2P" sul numero 15 di HJ e mi sono venute in mente varie domande. Monitorare quello che io faccio non è illegale in quanto violazione della privacy? Chi ci dice che hanno monitorato solo il P2P e non tutte le operazioni svolte da quei computer?
Per monitorare il traffico P2P non si dovrebberro sniffare i relativi pacchetti magari entrando nel computer in questione per metterci il "software realizzato ad hoc"?
Se utilizzo dei proxy o degli anonymizer o meglio ancora faccio la famosa "ragnatela di connessioni" (disponendo di una connessione in banda larga non mi rallenta molto) o uso il protocollo P2P in connessione secondaria, non posso sperare che perdano molto tempo a rintracciarmi o non mi rintraccino affatto (visto e considerato che dovrebbero passare a ritroso per una ventina di stati che non hanno nemmeno una polizia postale molto avanzata)?

Ruben

Non ti rispondo punto per punto, ma mi limito a una disquisizione generale.
Se monitorare quello che scarichi dai network P2P non è così facile, non è invece necessario mettersi a usare tecniche sofisticate per monitorare quello che _condividi_.
Basta effettuare la ricerca, vedere quali utenti hanno un certo file, mettersi in coda e –nel momento in cui cominci a scaricare– puoi vedere tranquillamente i loro indirizzi IP con un qualsiasi programma in grado di monitorare le connessioni TCP della tua macchina. Questo ovviamente a meno che, come indichi tu, non si sia usato un socks proxy.



Dicono che vengono in pace e portano dei doni...

DIALER WAP?

L'altro giorno stavo leggendo una rivista, naturalmente piena di pubblicità di suonerie e loghi che di solito ignoro... ma qualcosa mi è saltato all'occhio.
Una di queste pubblicità diceva: Download illimitato di loghi e suonerie, infatti bastava "solamente" inviare un sms ad uno strano numero +43699115***** (ometto giustamente le ultime cifre), e diceva che poi bastava salvare le impostazioni che ti arrivavano tramite sms per poter così navigare in un sito wap e scaricare senza limiti, l'inconveniente??? Costava 1.55 euro + IVA !!!
A questo punto mi chiedo: Ma non è anche questa una forma di dialer??? Basta salvare le impostazioni che arrivono per un sms e navighi a prezzi d'oro.
Boh, datemi un vostro parere.
Però una cosa la devo ammettere, sono stati onesti a mettere il prezzo in evidenza, cosa che non sempre accade.

Imperator

Anche se funziona in modo diverso dai dialer tradizionali, ne segue comunque la logica commerciale. Se però hanno messo in evidenza i costi, direi che non è il caso di incazzarsi più di tanto. Il problema sono quelli che vengono scaricati in automatico, e ti cambiano la connessione in modo permanente.
Ultimamente c'è anche una variante, che prevede l'invio di un SMS a tariffa premium. Rispetto ai dialer tradizionali, ha il vantaggio che la tariffazione non dipende dal tempo di connessione, ma è fissa e immutabile (un altro problema con i dialer è che spesso devi sfogliare numerose pagine prima di completare la procedura, e ogni secondo che passa lo devi pagare a caro prezzo).



Quella del "modding", ovvero la modifica del case dei computer ormai è una mania. Mandateci i vostri progetti e le foto delle vostre realizzazioni: li pubblicheremo in queste pagine.

MIGLIORE DEFINIZIONE

Vorrei un'esauriente definizione sul significato di hacker, i motivi per diventarlo (perché hacker si diventa) e i motivi per non diventarlo, cercando di essere il più chiari possibile.

Fox

Una definizione c'è a pagina 2 fin dal primo numero di HJ. Ma forse ti è sfuggita. Della distinzione tra hacker e criminali informatici se ne parla un numero sì e l'altro pure. Ma forse ti è sfuggito.
Il motivo per diventarlo… Vediamo. Qual è il motivo per cui uno decide di fare deltaplano? O immersioni subacquee? O dedicarsi all'ornitologia? La risposta è dentro di te, e in molti casi è sbagliata.
Il motivo per non diventarlo? Probabilmente la considerazione che, con un certo impegno e dedicandoci tutta la vita, forse è possibile conquistare Angelina Jolie o Sandra Bullock (Brad Pitt o Richard Gere per le nostre lettrici).

Saremo di nuovo in edicola 30 Gennaio!

VIOLARE LA POSTA

Nonostante sia un principiante di computer, compro sempre il vostro giornale, perchè mi affascina molto il pensiero di poter "entrare" nel computer di qualcun'altro.
Vorrei farvi qualche domanda:
Se io, su Hotmail, pigio su "hai dimenticato la password" e inserisco l'indirizzo di qualcun'altro e trovo la risposta alla domanda segreta e entro successivamente nell'account con la password che io ho messo, compio un reato? Cioè, sapete se ciò è legale?

Andrea

Secondo me compi almeno un paio di reati, e cioè l'intrusione in un account altrui e la violazione della corrispondenza privata. Lascia perdere e dedicati a qualcosa di più interessante.

DONO DELLA PREVEGGENZA...

Magari la domanda è idiota, ma mi chiedevo solo come mai, visto che mi collego solo oggi per la prima volta (vedi registrazione) e nella pagina di benvenuto ho scoperto di avervi visitato il 20/11/02 alle 10:07.
Siete dei paragnosti e prevedete il futuro (vi prego, datemi una mano col superenalotto) indovinando che ci sarei venuto nel forum oppura qualche figlio di mamma nubile ha rotto i coglioni a voi o a me, entrando al posto mio?

Giorgione

Hum… mi sa che in caso di nuovo utente il sistema prende come "data dell'ultima" visita quella di attivazione del database.

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: s3ga
pass: 9lla

☺☺☺ Tech Humor ☺☺☺

In rete circolano decine di storielle sugli utenti imbranati che telefonano al supporto tecnico. Ma che dire di certi tecnici che invece dovrebbero essere informati e preparati?

Mi sono ritrovato una vecchia scheda madre Compaq, che ho pensato di usare per assemblare un PC per mio fratello. Solo che non sapevo quale fosse la piedinatura del connettore di alimentazione (che non è standard). Ho chiamato il supporto tecnico, ed ecco la dicussione:
Io: "Ho una vecchia scheda madre Compaq 386 Deskpro. Ho bisogno di sapere qual è la piedinatura del connettore di alimentazione, in modo da poterla accendere e vedere se funziona".
Tecnico: "Hum... cosa succede quando accende il computer?"
Io: "Ma... niente. Non ho collegato l'alimentatore. Ho bisogno del significato dei piedini del connettore, per collegare un alimentatore standard"
Tecnico: "Capisco... ma riesce a entrare in Windows?"

Un giorno, accendendo il computer dell'azienda, questo ha cominciato a riavviarsi da solo non appena finiva il caricamento di Windows. Dopo una decina di riavvi, e non potendo usare un dischetto DOS per via di una protezione inserita dal responsabile informatico, ho deciso di chiamare il supporto. Dopo aver spiegato al tecnico cosa stava succedendo, la prima cosa che mi ha chiesto è stata: "Ma ha provato a riavviare il computer?".

Tecnico: "Siccome questo modem è plug-n-play, non può funzionare in Windows 3.11. Dovrà acquistare un nuovo modem oppure passare a Windows 95".
Cliente: "Ma ho usato questo modem con Windows 3.11 per più di un anno senza problemi".
Tecnico: "Ben, ora non funziona".
Cliente: "Ma se ha funzionato finora, perché non dovrebbe andare adesso?"
Tecnico: "Beh, potrebbe essere stato colpito da un fulmine, e qunidi ora può funzionare solo con Windows 95".

DIVX SULLA TV

Come posso far sì che il mio lettore DVD, cioè quello collegato alla televisione, legga i Cd che il mio masterizzatore sforna, contenenti film in formato DivX?

Jacques

I lettori domestici in grado di leggere DivX sono rarissimi: l'unico che conosciamo direttamente è quello di www.kiss-technology.com). Il modo più sicuro per far leggere un CD al lettore di DVD da tavolo è quello di masterizzarlo in formato VideoCD (ma, anche qui non tutti i lettori lo riconoscono, o se lo riconoscono magari non sono in grado di vedere un CD-R masterizzato). Il problema del VideoCD è che ha una qualità molto bassa e in un CD si riesce a malapena a far stare un'ora di video (quindi servono almeno due CD per un film). Alcuni lettori di DVD riconoscono anche i CD registrati in formato Super VideoCD (SVCD), che offre una qualità migliore ma una durata ancora minore di quella dei VCD (si arriva a 70 minuti circa solo diminuendo drasticamente la qualità). In sintesi, la soluzione migliore è quella di procurarti una scheda grafica con uscita TV per collegare il tuo computer al televisore di casa.

NEWS

HOT!

DEMO WI-FI DI COLT TELECOM

Colt sta procedendo a una serie di sperimentazioni di accesso wireless a Internet attraverso la tecnologia Wi-Fi. La prima è avvenuta (ed è tuttora operativa) presso l'Hotel Marriott di Milano, la seconda (e per ora ultima) presso la sede centrale di Roma delle Poste Italiane. Tali sperimentazioni stanno avendo luogo nell'ambito della preparazione al lancio dell'offerta al pubblico del servizio Wi-Fi di Colt Telecom.

AOL BREVETTA I MESSAGGINI

America On Line, attuale proprietaria di Icq, ha ottenuto il brevetto dell'instant messaging, richiesto nel 1997 da Mirabilis, l'azienda che ha inventato Icq. Ci sono tutti i presupposti per far tremare i polsi a più di una azienda, fra cui Yahoo! e Microsoft, anche se Aol afferma di non volerne approfittare in alcun modo. Anzi, pare sia già avviato da qualche tempo un progetto, in partnership con Microsoft, per lo sviluppo di sistemi di sicurezza per l'instant messaging aziendale.
Questo brevetto va ad aggiungersi ad altri già acquisiti da Aol, come quello sui cookie e su Ssl, su cui, ugualmente, Aol non ha mai esercitato alcun tipo di rivalsa.

SCUOLE MEDIE: ISCRIZIONI ONLINE

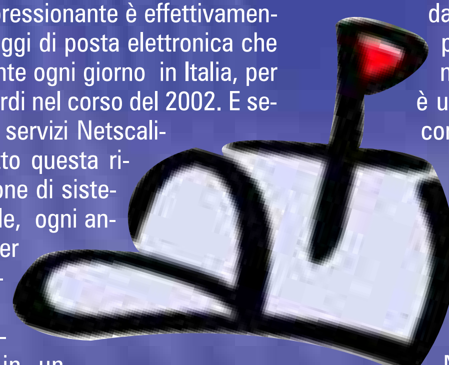
Dal 25 gennaio è possibile effettuare online le preiscrizioni al primo anno delle scuole superiori per tutti gli studenti che hanno terminato le scuole medie: lo ha reso noto il Ministero dell'Istruzione. Il sito di riferimento del Ministero è www.istruzione.it, e si garantiscono, naturalmente, gli adeguati supporti di sicurezza per il rispetto della privacy dell'utente.

PENSIONATI D'ASSALTO



L'ex responsabile (attualmente pensionato) dei sistemi informatici di una importante società finanziaria statunitense è stato accusato di aver danneggiato il server centrale della società stessa con una bomba logica; un virus a tempo, collocato evidentemente prima del suo pensionamento e che ha causato danni alla società per oltre tre miliardi di dollari.
Secondo gli inquirenti, lo scopo non era solo quello di compiere un gratuito vandalismo per pura vendetta (pare che l'uomo abbia dichiarato più volte di essersi sempre sentito tenuto in scarsa considerazione, soprattutto economica), quanto piuttosto quello di effettuare una spericolata speculazione, vendendo allo scoperto le sue azioni in previsione del calo dovuto al crash del sistema. Ma il calo non ha avuto luogo, e le inchieste hanno portato a individuare il colpevole nel neopensionato.
Le sanzioni non si prospettano troppo clementi: dieci anni di reclusione per ciascuno dei due capi d'accusa, frode nella gestione dei sistemi di sicurezza e frode finanziaria realizzata mediante l'uso di strumenti informatici, e la possibilità di una multa oltre il milione di dollari.

200 MILIONI DI EMAIL AL GIORNO



Questo numero impressionante è effettivamente quello dei messaggi di posta elettronica che circolano mediamente ogni giorno in Italia, per un totale di 70 miliardi nel corso del 2002. E secondo la società di servizi Netscalibur, che ha condotto questa ricerca su un campione di sistemi di posta aziendale, ogni anno circola il 25 per cento di posta elettronica in più rispetto all'anno precedente. Questo in un quadro complessivo di 4000 miliardi di email in un anno nel mondo, dieci volte tanto gli Sms, dato che potrebbe far alzare un sopracciglio ai fanatici diteggiatori, ma è proprio così (del resto il Sms è un fenomeno tipicamente italiano, con pochi emuli nel resto d'Europa).Si è anche calcolato che, in media, ogni utente Internet scambia 70 messaggi al giorno, impiegando circa due ore della propria giornata lavorativa, numero che però è destinato a crescere nel periodo attorno a Natale. Infatti si pensa che il numero di messaggi quotidiani toccherà e forse supererà il miliardo.

MUSICA VULNERABILE

Windows XP e WinAMP sono soggetti ad alcune vulnerabilità di sicurezza relative alla gestione degli attributi dei file audio. A causa di ciò, l'esecuzione di file Mpe o Wma creati ad hoc da un malintenzionato potrebbe compromettere seriamente l'integrità del sistema. Senza contare che, una volta che questi file dovessero entrare nel circuito del file sharing, il problema si moltiplicherebbe all'infinito.
Attualmente anche gli utenti meno smaliziati diffidano di un allegato di posta elettronica eseguibile, ma nei confronti dei file audio non c'è nessun genere di diffidenza, cosa che peggiora ulteriormente le cose.
Tecnicamente, la falla risiede, per quanto riguarda Media Player, in un buffer overflow presente nella funzione che permette a Explorer di interpretare gli attributi dei file Mp3 e Wma, ivi comprese tutte le informazioni relative a anno di produzione, autore, titolo, durata del brano e bit rate. Basta quindi il semplice passaggio del mouse per eseguire il comando incriminato, nascosto fra le tag informative sopra citate; non c'è nemmeno bisogno di aprire o selezionare il file contaminato! Per WinAmp, la stessa cosa accade con le tag Id3v2. Sono comunque disponibili le relative patch sui siti di Microsoft e di NullSoft.

HACKER STUDIOSI

Uno studente modello di un liceo californiano ha preso molto sul serio la concessione datagli dal preside della sua scuola, al quale aveva chiesto di poter sperimentare praticamente, sul sistema informatico della scuola, le tecniche apprese in un corso sulla sicurezza informatica. Negli Stati Uniti i registri sono elettronici, e i voti vengono registrati nel server scolastico; molti sono, quindi i tentativi di intrusione. Di conseguenza, le scuole vigilano parecchio sulla sicurezza del sistema, soprattutto per quanto riguarda la possibilità di intrusioni dall'esterno. Lo studente in questione è riuscito ugualmente a entrare nel sistema, ma, avendo il massimo dei voti in tutte le materie, è riuscito solo a abbassarsi tutte le valutazioni. Rischiando, così, di dover mantenere tali mediocri votazioni, in quando il preside, certo dell'inviolabilità del sistema scolastico, ha fatto passare sotto silenzio l'accaduto, bloccando il sistema fino a quando i liveli di protezione del server scolastico non sono stati alzati.

GOOGLE DANCING

Avete ottenuto risultati contradditori da una stessa ricerca effettuata in tempi diversi su Google e vi state chiedendo dove avete sbagliato? Niente paura, è colpa di Google e della sua... passione per il ballo.
La Google Dance è un fenomeno che porta le pagine inserite nel noto motore di ricerca a "danzare" periodicamente, ovvero a cambiare frequentemente posizione del ranking da un periodo all'altro, e in certi casi ad uscirne del tutto. Ciò avviene per via della presenza di ben 7 centri di elaborazione dati, distribuiti sul oltre 10.000 Pc sparsi in mezzo mondo, che sono aggiornati con frequenze differenti. Nel corso delle imponenti reindicizzazioni del sistema, quindi, il nostro risultato quindi cambierà a seconda del datacenter interrogato, che potrà essere alternativamente il più vicino o quello con minor carico di lavoro.
Ci sono imponenti documenti in rete che insegnano a sfruttare la Google Dance per far salire le proprie pagine nel ranking, o semplicemente a seguire questa complessa procedura, tracciando Dns a caccia dei risultati più aggiornati all'interno della folle danza di Google.

COPIARE DVD È LEGALE IN ITALIA

LI programmi per eseguire una copia da Dvd, rigorosamente vietati negli Stati Uniti, saranno invece messi in libera vendita in Italia, con tanto di beneplacito della SIAE, in base al principio per cui è assolutamente lecito eseguire una copia di backup di un supporto magnetico o ottico.
Questo in barba alle protezioni anticopia poste sui Dvd, che dovevano essere un baluardo insormontabile (almeno a parere delle major cinematografiche) e che vengono invece tranquillamente (e a pieno diritto) infrante da questi software.
Non che nessuno avesse mai provato prima a copiare un Dvd in Mpeg e convertirlo in DivX, questo è chiaro. Probabilmente questi sistemi si baseranno sulle stesse tecniche, ma non sarà più, finalmente, qualcosa di complesso e riservato agli addetti ai lavori. Con questi software chiunque potrà scegliere il formato di codifica, la compressione, e in generale effettuare la duplicazione esattamente come oggi si duplica un normale Cd-Rom.

HOT!

SSH BUCHERELLATO

Diverse implementazioni del protocollo SSH (fra cui non figura OpenSSH) sono soggette a serie vulnerabilità (le famigerate "buffer overflow"), che potrebbero creare basi per attacchi DoS o addirittura concedere ad un aggressore di prendere il controllo di una macchina, eseguendo in remoto codice con gli stessi privilegi di SSH (quindi root).

FALLA IN FLASH

E' stata riscontrata un serio problema di sicurezza nell'ormai universalmente diffuso plugin Macromedia per la visualizzazione delle animazioni su Web: una pagina appositamente predisposta potrebbe generare l'esecuzione di codice sulla macchina locale, con danni non indifferenti, che potrebbero comprendere la cancellazione di dati o anche la formattazione dell'intero disco fisso. La patch, neanche a dirlo caldamente consigliata, è disponibile sul sito Macromedia.

FLAT GPRS DA ARUBA

Aruba lancia un'offerta decisamente accattivante, denominata "Aruba Gprs Flat", che permette di connettersi via Gprs ad un costo fisso mensile di 28,00 Euro (+Iva), indipendentemente dal tempo di connessione e dal traffico in Kbyte (quest'ultimo da sempre l'unità di misura della connettività Gprs). In questi termini, la connessione Gprs può essere finalmente utilizzata a tutti gli effetti in sostituzione di una connessione tradizionale.



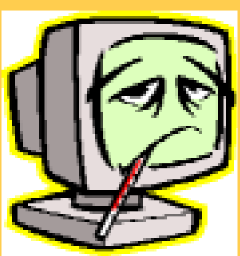
HOT!

FIBRE OTTICHE AI FOTONI

Suona come qualcosa che esce direttamente da un romanzo di fantascienza, ma si tratta invece di uno studio molto serio, in corso ad Oxford, e che potrebbe rivoluzionare il mondo della connettività. Pare infatti che un nuovo tipo di cristallo fotonico potrebbe sostituire i dispositivi elettronici usati per instradare i segnali nelle reti di comunicazione a fibre ottiche. Il differente materiale impiegato consentirebbe di raggiungere velocità di trasmissione maggiori e dispositivi di dimensioni molto più contenute.

L'INVASIONE DEI VIRUS

Message Labs, una società inglese che si occupa di filtraggio della posta, ha reso note le statistiche relative ai virus presenti nei messaggi di posta elettronica. In due anni, la percentuale di messaggi infetti è passata dallo 0,2 % allo 0,6%, cioè in pratica un messaggio infetto ogni 200, un numero inquietante, vista la mole di posta elettronica processata ogni giorno dalla società: circa 10 milioni di messaggi. In termini di tempo, ogni tre secondi viene bloccato un messaggio contaminato da virus. E il record di frequenza è di Klez.H., mentre quello di velocità di diffusione è di Bugbear.



"ANALIZZANDO E VALUTANDO TUTTE LE IDEE, HO CAPITO CHE SPESSO TUTTI SONO CONVINTI CHE UNA COSA SIA IMPOSSIBILE, FINCHÉ UN GIORNO ARRIVA UNO SPROVVEDUTO CHE NON LO SA E LA REALIZZA"

(Albert Einstein)

GOOGLE SI SPECIALIZZA

Google, che attualmente si può fregiare di essere il motore di ricerca più utilizzato al mondo, ha recentemente lanciato due motori specializzati: Google News, dedicato alle notizie, e, in occasione della febbre per lo shopping che da sempre accompagna il periodo natalizio, Froogle.

Google News raccoglie automaticamente, ogni giorno, le notizie più importanti da circa 4000 fonti diverse, e l'aggiornamento è effettuato in tempo reale, con le notizie più recenti in alto e via a scendere. Ogni notizia è ricavata da fonti diverse, con relativo link, per un facile confronto. Tutto il processo è completamente automatizzato, senza alcun intervento umano.

Froogle è basato sia sui dati raccolti in modo tradizionale da Google che sulle inserzioni a pagamento delle aziende, che possono acquistare parole chiave ma che ad ogni modo, per correttezza, vedranno i loro link visualizzati in maniera distinta, come già accade per l'edizione "normale" di Google. Ogni prodotto ha un link ai rivenditori, il prezzo e, se disponibile, una immagine che lo raffigura.

MULTE PER LO SPAM MULTI LIVELLO

Chi non ha ricevuto, prima o poi, almeno una di quelle email che promettono denaro facile lavorando via Internet, in una qualunque delle tante versioni, tutte riconducibili al MLM (Multi Level Marketing)?

Molti avevano chiesto a gran voce un modo per bloccare il fenomeno, che aveva assunto proporzioni preoccupanti (soprattutto per il numero di persone che sembravano disposte a credere in quell'assurdo miraggio).

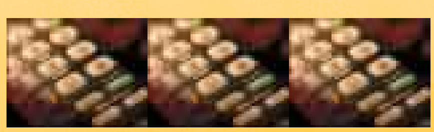
Già, perché, nonostante i rassicuranti disclaimer presenti nel corpo del messaggio, che assicurano che è spamming sì, ma a norma di legge, l'iniziativa è non solo molesta ma, per le leggi italiane, ai limiti della legalità.

Ora qualcosa si sta muovendo: uno dei mittenti di questo tipo di spam, che per il meccanismo stesso con cui è costruito il sistema MLM non nasconde i suoi dati come lo spammer medio, anzi, ne dà piena pubblicità, è stato punito con una multa di 250 euro per non aver saputo giustificare la lecita provenienza di un indirizzo di un cittadino che si era giustamente lamentato presso il Garante per la Privacy Finalmente qualcosa si muove nella lotta allo Spam.



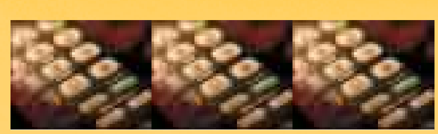
LE TELEFONATE PIÙ CARE D'EUROPA

I giornali, le riviste, i palinsesti televisivi sono letteralmente infarciti di pubblicità di offerte riguardanti la telefonia cellulare, e noi, attorniati da carte di Natale e autoricariche, ci sentiamo dei privilegiati. Nulla di più sbagliato. I nostri provider di telefonia sono stati severamente bacchettati dal Garante per le Telecomunicazioni inglese, che ci ha mostrati a dito come il paese con i cellulari più costosi d'Europa.

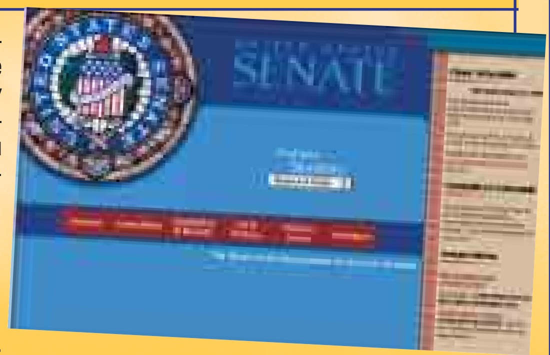


Il conto è presto fatto: i cellulari costano di più, ci sono più tasse e le tariffe sono più alte (in media, persino le offerte promozionali sono più alte del 27% di quelle più care nel resto d'Europa). Anche il roaming non è precisamente economico, più caro, in questo caso, di circa il 20%.

L'Authority italiana, di fronte a questi dati, si trincera dietro a un silenzio suggellato da una affermazione anche troppo ripetuta, "per ribassare le tariffe si attendono iniziative a livello europeo".



SENATO ANONIMIZZATO



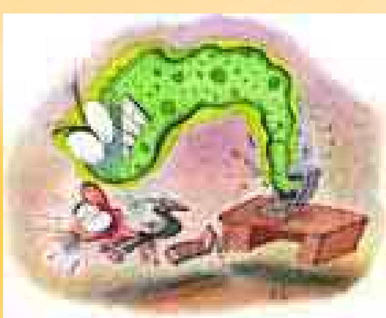
Il sito del Senato statunitense, www.senate.gov, ha svolto per mesi involontaria funzione di anonimizzatore gratuito, attraverso un proxy server pubblico (opportunamente chiuso in tutta velocità) che permetteva ai navigatori più smaliziati di nascondere le proprie tracce, facendole puntare ad un sito al di sopra di ogni sospetto.
Questo proxy sarebbe stato normalmente adibito a gestire le richieste Web da parte degli utenti della rete interna verso l'esterno, ma per via di un errore di configurazione tali richieste potevano essere effettuate anche da parte di utenti esterni alla rete. Pare che però la vulnerabilità si limitasse all'utilizzo del proxy: la rete interna, secondo le dichiarazioni dei responsabili, è sempre stata adeguatamente protetta.
Il punto debole è stato scoperto da un hacker, volutamente andato a caccia di eventuali falle in un sito così importante come quello del governo statunitense.

UN WEB PER TUTTI



E' stata presentata, nel corso di un convegno sui diritti della Rete, una proposta di legge che stabilisce il diritto di accesso alle risorse telematiche ai disabili, con tanto di salatissime sanzioni per chi non adegua le proprie strutture, rendendole pienamente accessibili.
La proposta è stata illustrata nel corso del convegno IWA "Internet: un diritto per tutti" tenutosi a Venezia. L'intenzione non è quella di stabilire nuovi standard, ma di richiamare l'attenzione su quelli già esistenti e sanciti dal World Wide Web Consortium, che purtroppo non sempre vengono tenuti in considerazione dai webmaster. E se la mancanza è veniale per i siti generici, diventa inammissibile quando si parla di siti di servizio o di pubblica utilità.
In otto articoli vengono definite le risorse pubbliche e di pubblica utilità, gli obblighi delle pubbliche amministrazioni in merito e gli strumenti telematici per agevolare l'integrazione dei lavoratori disabili. Speriamo che queste regole vengano prese sul serio dai webmaster, soprattutto da quelli che operano nel settore pubblico.

ATTACCHI MILITARI E TELEMATICI



Al Quaeda, la famigerata organizzazione terroristica capeggiata da Osama Bin Laden, non conta soltanto terroristi, diciamo così, "tradizionali", ma anche cracker che si dichiarano pronti a rispondere a un eventuale attacco statunitense in Iraq con una controffensiva telematica. Uno di loro, noto come "Melhacker", che si dichiara membro di al Quaeda con il nome di battaglia di Nur Mohammad Kamil, è un creatore di virus piuttosto noto:pare abbia già diffuso in rete diversi worm e virus fra cui VBS.OsamaLaden@mm, Melhack, Kamil, BleBla.J e Nedal. E i nomi dei virus mostrano senza troppi dubbi l'orientamento delle sue simpatie, se ce ne fosse bisogno, senza contare che pressoché tutti contengono riferimenti alle "imprese" del gruppo terroristico, 11 settembre compreso.
La minaccia non è da prendersi a cuor leggero: il cracker ha rivelato di avere pronto da tempo un temibile Worm, denominato Scezda, costruito assieme a sul modello di SirCam, Klez e Nimda, ma con effetti più devastanti.

HOT!

IL RITORNO DELLE FLAT

Edisontel propone una soluzione molto interessante, in alternativa all'Adsl, per chi non è coperto dal servizio a larga banda o semplicemente ha esigenze di mobilità o di sottoscrivere servizi a breve durata. Il contratto, denominato WooowFlat, mette a disposizione degli utenti una casella di posta elettronica da 10 Mbyte e la connessione abilitata 7 giorni su 7, in qualunque fascia oraria, a un canone fisso mensile di 33,06 euro per collegamento Pstn, 36,72 euro per Isdn 64 kbp/s e 73,44 euro per Isdn 128 kbp/s (con abbonamento annuale).

ALICE È PRONTA



Intel e Telecom Italia hanno stipulato un accordo per presentare sul mercato "Alice Ready", un Pc con Pentium 4 e modem ADSL preinstallato, e naturalmente una connessione Alice ADSL.
con varie velocità, fino a 1,2 Mbit/sec).
Questa iniziativa riprende quella già tentata con E-vai da Telecom Italia circa tre anni fa, che prevedeva l'offerta di un Pc dotato di abbonamento Tin.it, ma allora su normale linea telefonica commutata.

FOTOGRAFARE CON PALM



È da pochi giorni sugli scaffali dei negozi Veo SD Photo Traveler, una piccola fotocamera digitale per Palm OS, compatibile con tutti i modelli che dispongono di slot di espansione Secure Digital del palmare. L'utilizzo è semplicissimo: basta introdurla nello slot ed è già operativa. Le fotografie sono a colori a 24 bit, a 640x480 pixel, in formato JPEG, con autoscatto e preview dell'immagine in tempo reale, e visualizzazione delle thumbnail delle immagini scattate. Il costo è di 129 Euro (Iva inclusa).

VITA, PAURE E PROFEZIE DI UN VISIONARIO DEL WEB

IL MONDO FINIRÀ IN UN BIT

Dagli editor di testo ai file system, dall'architettura dei processori al linguaggio Java, Bill Joy ha messo lo zampino un po' in ogni tecnologia importante negli ultimi trent'anni. E ora avverte: presto le macchine potrebbero dominare il mondo



Bill Joy, co-fondatore della Sun Microsystems e grande programmatore, come molti scienziati moderni, ha un rapporto ambiguo e contraddittorio con la tecnologia. Nel corso della sua vita è stato continuamente **impegnato nella ricerca di software sempre più avanzati, in grado di muovere le "macchine"**, ovvero i computer, al servizio dell'uomo. Ma da qualche anno la sua mente di visionario corre oltre, **vede un mondo che fra pochi anni, precisamente nel 2030, sarà dominato non più dagli uomini ma da robot e mutanti**. Il profeta del Web ha affermato di essersi trovato, suo malgrado, a condividere una tesi di "Unabomber", al secolo Theodore Kaczynski, il famigerato eco-terrorista arrivato ad uccidere per protesta contro la tecnologia.

"Ho sempre pensato che facendo software sempre più affidabile, avremmo creato un mondo più sicuro", dice Joy. "E che se fossi arrivato a pensare il contrario, avrei avuto l'obbligo morale di fermare questo lavoro. Ora posso immaginare che questo momento verrà".

>> L'apocalisse secondo Bill

L'ideatore di Java e Jini ha anche guidato nel 2000 una commissione presidenziale sul futuro delle nuove tecnologie e il suo avviso ha **lo stesso scopo della lettera che Albert Einstein scrisse nel 1939 al presidente Franklin Delano Roosevelt sui pericoli della bomba atomica**. Secondo il padre di Sun, in un futuro molto vicino, **i robot supereranno gli esseri umani in intelligenza** e potranno replicare se stessi. I progressi della nanotecnologia porteranno a **macchine così piccole da poter entrare in un vaso sanguigno**. Mentre la tecnologia genetica sta inesorabilmente generando il potere di creare nuove forme di vita in grado di riprodursi. Tutto questo può avere risvolti catastrofici: le nuove tecnologie creano il potenziale di nuove piaghe meccaniche e biologiche auto-replicanti e mutanti.



Jim Gosling, co autore di Java, disegna con una torcia il contorno di una tazzina di caffè, simbolo del sistema operativo.

"Immaginate un attacco sul mondo fisico, sul modello dell'attacco con cui i cracker possono mettere in ginocchio un sito web, paralizzandolo del tutto", afferma Joy. E, a suo giudizio, **i rischi di un'apocalisse in un futuro imminente sono molto più grandi di quelli legati alla bomba atomica**. "Le nuove tecnologie sono a basso costo: per questo a differenza della bomba atomica i problemi potrebbero venire non da governi malintenzionati, ma da singoli individui".

A spaventarlo non sono comunque le nuove tecnologie in senso lato, ma il loro cattivo utilizzo.

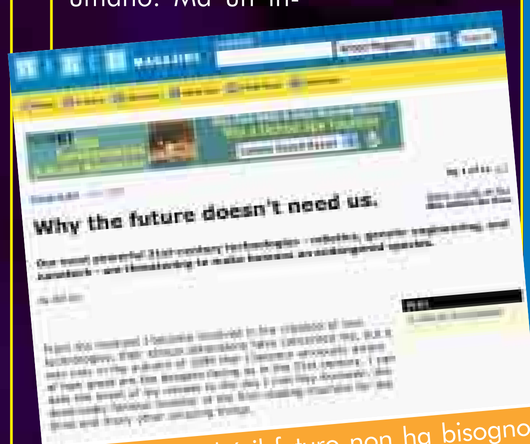
>> Non solo paranoia

È un grande sostenitore dell'open source e del peer-to-peer – dei quali è stato un pioniere - ma al contempo non si esime dal criticarne i difetti. "Sun è da sempre sostenitrice dell'open source", sostiene Joy - la causa intentata contro Microsoft ne è una prova lampante – "ma non significa che questa filosofia abbia generato sino ad oggi programmi per forza migliori". Anche il peer-to-peer nasconde qualche insidia, soprattutto nella sua ottica negativa: insieme ai file "normali" e puliti si possono distribuire anche le bombe della Rete, rappre-

sentate dai temibili virus.
A parte le ossessioni tecnologiche, la storia del guru non è fatta solo di timori e nemici impossibili, tutt'altro. Già vent'anni fa pensava a un software che permettesse di creare programmi in grado di girare su ogni piattaforma, da una scheda con chip a un grande sistema. Dopo averlo elaborato gli mancava solo **un nome che gli venne pensando ad una famosa qualità di caffè: Java.**
Definito come l'innovazione informatica più importante degli ultimi anni, il linguaggio universale ha trovato una fondamentale applicazione nei siti Internet, e dopo qualche anno, è stata pensata anche una sua versione per ogni strumento portatile, dal nome Jini.

>> Nel frattempo, a Redmond...

Tutto questo successo non è piaciuto ad un altro Bill (Gates), poiché Java mina alle radici ogni standard proprietario. **Il fondatore di Microsoft ha pensato di boicottare il linguaggio universale nei software prodotti dalla casa di Redmond**.
Anche la Sun si è quindi accodata all'ondata di cause che sono state intentate contro la Microsoft chiedendo, nel marzo 2002, oltre un miliardo di dollari di danni per "estesa condotta anti-competitiva".
Nel processo, da poco iniziato, la Sun Microsystems ha chiesto alla Corte distrettuale di Baltimora di imporre alla Microsoft l'inclusione dei codici di Java in tutte le copie del sistema operativo Windows. L'azione ha carattere del tutto preventivo: data la probabile lunghezza del procedimento, infatti, Sun ha pensato di **ottenere un provvedimento temporaneo che costringa Microsoft, già prima della sentenza definitiva, a ospitare nel proprio sistema i codici del software di Sun**. La causa avanzata dall'azienda americana arriva ad alcune settimane dalla contestata decisione della Corte di Washington di avallare l'accordo raggiunto tra la Microsoft e l'amministrazione Bush proprio in ambito di lesione della concorrenza.
Per il momento, quindi, il grande nemico di Bill Joy non è un futuro alla Blade Runner, costellato di androidi pronti alla rivolta contro il genere umano. Ma un in-


Why the future doesn't need us.

L'articolo "Perché il futuro non ha bisogno di noi", col quale Bill Joy mette in guardia contro i possibili risvolti negativi delle più recenti tecnologie. Undici fitte pagine da leggere con calma, all'indirizzo www.wired.com/wired/archive/8.04/joy.html

dividuo che tutti conoscono molto bene: Bill Gates. Con il quale ha da spartire solo il nome. **Joy, infatti, ha mantenuto intatto, come Steve Wozniak, Steve Jobs e altri, lo spirito dell'università californiana degli anni settanta**, dove l'informatica era diventata il surrogato della contestazione giovanile.

>> Un geek di 50 anni

Mentre Gates si è gradualmente trasformato in un abile e scaltro imprenditore, gli altri, pur diventando anch'essi milionari, hanno mantenuto intatta la visione critica della realtà tecnologica. **Joy sfoggia ancora, a 48 anni, lunghi capelli e occhialini da nerd**, dopo aver fondato, nel 1982, la Sun Microsystems, non ha riflettuto troppo sul fatto di vendere gran parte delle azioni e "fuggire" dalla Silicon Valley, aprendo un laboratorio sulle cime di Aspen, in Colorado. E proprio durante il suo "eremitaggio", fra le Montagne Rocciose e il lago Tahoe, che la sua creatura, Java, ha preso forma. E da qui è partita, sempre a capo della sua Sun, l'ultima grande offensiva contro i nemici di Redmond. Si tratta del progetto **open source JXTA, una piattaforma peer-to-peer che, mediante Java, ambisce a divenire uno standard aperto**.
Simile a Napster e Gnutella, il progetto è comunque più vasto e ambizioso: il suo fine è quello, infatti, di utilizzare il peer-to-peer nelle più diverse operazioni online come ricerca di informazioni, download, streaming e anche fruizione di servizi. E JXTA non si limita ai soli PC ma rende interoperabili fra loro telefoni cellulari, PDA, set-top box, computer desktop, server. **In un anno dalla sua presentazione, il progetto vede la partecipazione di 10mila ricercatori** e l'interesse delle maggiori aziende del settore computing e entertainment. Il convitato di pietra è naturalmente sempre lui: Gates.

Alessandro Carlini

Bill Joy in breve

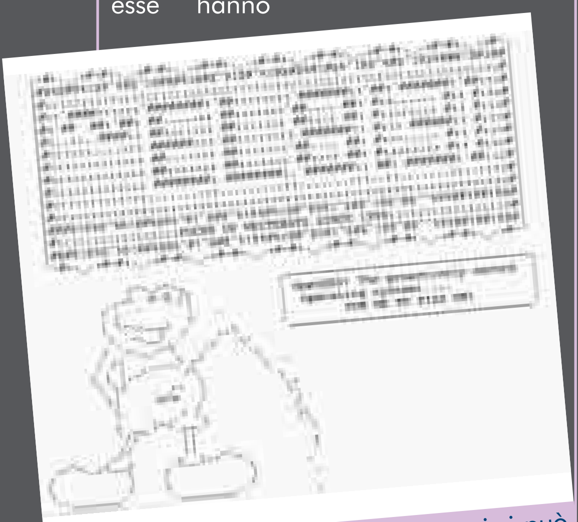
Alla fine degli anni '70, Joy si trova nel posto giusto al momento giusto: alla Berkeley Universiti. Lì scrive la prima versione dell'editor di testo vi, e sviluppa gran parte di BSD, la distribuzione Unix della Berkeley, appunto. Per Sun, azienda in cui ricopre incarichi dirigenziali fin dalla fondazione, ha progettato (o contribuito a progettare) gran parte delle tecnologie-chiave dell'azienda: Network File System (NFS), l'architettura dei processori UltraSparc. Il suo lavoro su Java è forse sovrastimato (a questo linguaggio ha lavorato molto di più James Gosling, altro pezzo grosso di Sun fin dagli esordi).
Attualmente, in Sun ricopre l'incarico di "Chief Scientist and Corporate Executive Officer", dimostrando che anche nelle cariche ci vuole un pizzico di originalità.

UN BEL FILM DIVENTA UN BRUTTO INCUBO PER GLI ESPERTI DI SICUREZZA

pr0jekt m4yh3m

Non prendiamoci in giro: gli hacker cattivi esistono, e ora si stanno anche organizzando.

Da qualche mese a questa parte, i più noti White Hat (gli hacker "etici") e gli esperti di sicurezza sentono il fiato sul collo. Un manipolo di hacker di quelli tosti, li ha presi di mira. Obiettivo: **possedere le loro macchine, ridicolizzarli, infrangere il mito dell'hacker con una coscienza**. Stiamo parlando del "Progetto Mayhem", lanciato da una persona (o un gruppo) che si firma ~el8 e che nella sua una ezine **incita il mondo hacker alla rivolta contro chi si occupa di sicurezza informatica**.
Gli attacchi diretti proprio alle società che si occupano di sicurezza non sono poi una novità: già in passato alcune di esse hanno subito attacchi (principalmente di tipo Denial of Service), ma in passato si è sempre trattato di qualche script kiddie che si è trovato tra le mani questo o quello strumento di attacco. In questo caso, invece, gli attaccanti hanno dimostrato di sapere ciò che stavano facendo. **Si tratta di persone preparate e determinate, che studiano il loro bersaglio per molto tempo, per poi colpirlo la dove fa più male: la loro directory root.**



Se non li si prende troppo sul serio, ci si può anche divertire a leggere alcuni passi delle ezine qui citate.

>> La ezine di ~el8

Le ezine diventa quindi il modo per dimostrare di aver violato alcuni dei computer che si suppongono essere i più sicuri al mondo. Nel testo si trovano infatti le email e i file personali delle vittime, liste di utenti e processi attivi, e ogni altra prova della avvenuta violazione. Insieme a deliranti minacce e dichiarazioni di intenti: **"Perché scegli di diventare nostro bersaglio quando potresti unirti a noi? Perché diffondere informazioni, codici o bachi quando il risultato finale è che il tuo intero sistema, la tua famiglia e i tuoi amici saranno posseduti? Non è 100.000 volte meglio essere un Black Hat invece che un White Hat? (Non c'è via di mezzo)"**. E ancora: "Siamo gli hacker hardcore che puliscono i tuoi bagni, i coder che insistono nel pulire i vetri della tua auto agli incroci, gli hardcore phreaker che tagliano la tua erba, i cracker che rubano i vestiti dai cassonetti dell'esercito della salvezza. Prendiamo i tuoi ordini al Burger King… NON CERCARE DI FREGARCI!". Ci sono anche istruzioni per gli adepti: **"Pensi di andare a DefCon o BlackHats (le due più famose convention hacker)? Colpiscili col Napalm!"**. "Vivi vicino a un'azienda di sicurezza? Spara agli impiegati con



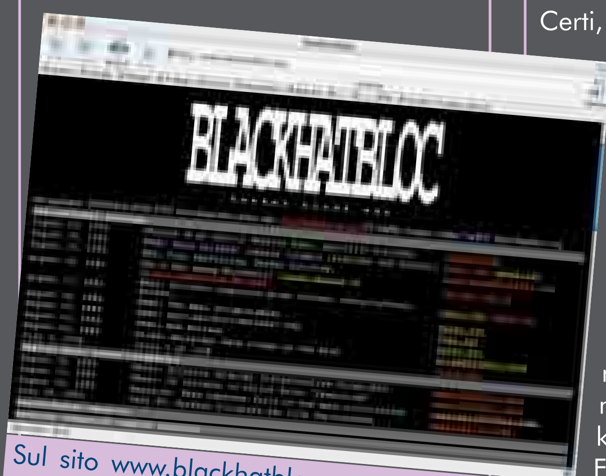
pistole a vernice, picchiali e minacciali". E poi liste di siti da bersagliare con attacchi DoS: Securityfocus, Google, Packetstorm, Freshmeat, Slashdot, Cnn, solo per citarne alcuni.

>> E non sono i soli...

Ma gli attacchi alla comunità della sicurezza e agli hacker etici non vengono da una parte sola: accanto al progetto Mayhem ci sono anche le missioni del "Phrack High Council", Gobbels e altri gruppi "anti white hat". Contrariamente a quanto potrebbe far pensare il nome, il Phrack High Council (PPHC) non ha nulla a che vedere con la celebre ezine Phrack (www.phrack.org) e, anzi, proprio Phrack rappresenta uno dei principali destinatari dell'odio del PHC. Come negli altri casi, Phrack sarebbe colpevole di "lavorare per il nemico", fornendo informazioni sui bachi dei sistemi e sui codici di exploit. Il gruppo si ritrova sul canale #phrack di EFNet

>> Una comunità in subbuglio

Le azioni dei vari gruppi anti white-hat hanno suscitato reazioni piuttosto varie nella comunità degli hacker etici e degli esperti di sicurezza. Qualcuno ha gridato subito all'attentato terroristico, chiedendo azioni rapide dell'FBI e punizioni severe da parte della giustizia americana. E dopo l'11 settembre, quando qualcuno grida "dagli al terrorista", sicuramente non viene sottovalutato. Altri sostengono che converrebbe evitare addirittura di parlare di questi attacchi: del resto, questi scalmanati si nutrono dell'attenzione che i



Sul sito www.blackhatbloc.org, si possono trovare i mirror dei siti di ~el8, Phrack High Council e altri (cosa più che mai utile, visto che i siti originali rimangono su pochi giorni prima di venire rimossi...).

media e la Rete riserva a loro e alle loro azioni. Per questi secondi osservatori, se li si ignora, dovrebbero stancarsi facilmente del loro giochino.
Qualcun altro, però, con un sorriso un po' sornione, fa notare come il Progetto Mayhem stia pungendo nel vivo quegli hacker che forse hanno perso di vista gli obiettivi iniziali di conoscenza e libertà, e hanno cominciato a vendere i propri servigi proprio alle aziende che una volta tanto criticavano. Hacker che sono riusciti a farsi accettare dalla società, e ora sono terribilmente irritati da questi illustri sconosciuti che gli fanno fare brutta figura con i loro clienti e che gridano, ancora una volta, che "il re è nudo".
Certi, pur non condividendo i metodi dei "black bloc digitali", fanno però notare che il fatto di distribuire pubblicamente le informazioni, non fa altro che fare arricchire certe neonate aziende di sicurezza, che utilizzano gli stessi tools dei cracker per individuare e rimuvere le falle di un sistema, senza necessariamente avere una conoscenza molto approfondita dell'argomento (chiamteli "script security kiddies", se volete).
Fatto sta che anche i veterani del settore, ci si scambia battutine su cosa sia più etico: non avere etica, essere hacker in vendita, o semplicemente collaborare col "nemico". Per esempio, suona piuttosto sibillina una frase che si trova nell'introduzione del numero 8 della nostrana ezine OndaQuadra (www.ondaquadra.org): "Avete scritto un articolo fantastico, estremamente complesso, dove viene illustratta una nuova sofisticatissima tecnica? Mandatelo a Bfi (o a phrack o alla Microsoft, è uguale) :)"



Il "Progetto Mayhem" è il piano che anima i protagonisti del film Fight Club, con Brad Pitt e Edward Norton, uno dei più
fine dello scorso millennio. In questo caso, Mayhem (mutilazione, storpiamento) è la distruzione, ottenuta con gli esplo
sedi delle principali banche e istituti di credito, che nelle intenzioni dei cospiratori avrebbe azzerato tutti i debiti e i cred
tando l'umanità a uno stato primordiale e a una società anarchica. Non è solo il nome del progetto a richiamarsi al
anche molte delle frasi e dei motti riportati nella ezine di ~el8. C'è da sperare che gli adepti del progetto non si pren
serio quando scrivono: "Non vogliamo più che voi, nostri fedeli seguaci, vi limitiate a possedere i sistemi degli esperti d
za che vi capitano a tiro. Vogliamo che voi provochiate la distruzione fisica dell'intera infrastruttura della sicurezza mon

COME FUNZIONA LA CODIFICA SATELLITARE



Il cielo in una stanza

Per chi si avvicina al mondo delle TV satellitari, il primo ostacolo è spesso rappresentato da un gergo piuttosto complicato e dalla poca chiarezza sui meccanismi di autenticazione e cifratura.

Ultima ora: anche Seca 2 è stato violato!
Tutti i dettagli a pag. 16

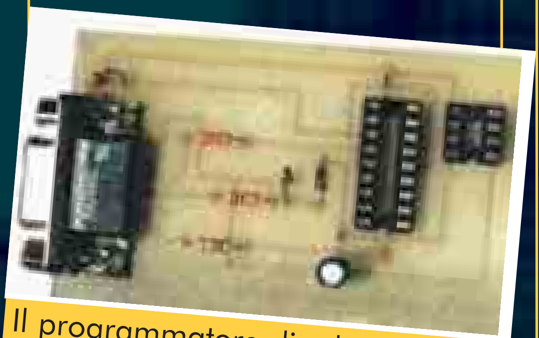
Un satellite altro non è che un ripetitore: riceve un segnale da un punto sulla terra e lo ritrasmette in un altro. Il collegamento da terra verso il satellite è detto up-link, mentre quello dal satellite verso terra down-link. Negli ultimi anni si è assistito ad un vero e proprio boom della trasmissione satellitare grazie alla diffusione di canali televisivi trasmessi, appunto, via satellite. In Europa per la trasmissione digitale sono seguite le raccomandazioni DVB (Digital Video Broadcast).
Lo standard DVB definisce le specifiche per la trasmissione televisiva digitale in generale (non solo via satellite), infatti, esistono differenti documenti per i diversi canali trasmessi. Il DVB-S descrive il protocollo della trasmissione via satellite, il DBV-T tratta quella dei canali digitali terrestri, mentre il BVD-C si occupa del via cavo. **Esistono principalmente sei sistemi di codifica**, utilizzati dalla maggior parte dei provider europei e non: sono l'Irdeto, il Seca, il NDS, il ViAccess, il CryptoWorks ed il PowerVu. In Italia attualmente ci sono due provider: Tele Più e Stream.



>> Apparecchiatura

Per vedere la tv satellitare dopo aver montato la parabola e l'illuminatore (l'installazione di un riflettore parabolico per la ricezione televisiva da satellite non presenta oggi eccessivi problemi, considerata la notevole potenza dei trasponder a bordo degli attuali satelliti) bisogna collegare il decoder, ma qual è il migliore? Qual è il più affidabile? Innanzi tutto dipende dalle vostre esigenze, sul mercato se ne trovano d'ogni tipo, marca e prezzo!Prima dell'acquisto di un decoder, dovreste, prima di tutto chiedere di che tipo di **CAM (Modulo d'accesso condizionato**, è la parte del decoder in grado di rimettere in chiaro il segnale criptato) è dotato, non potete comprare un Gold Box per vedere Stream. Stream necessita di un decoder Italtel Stream oppure un Common interface con CAM Irdeto. Altra soluzione è di comprare appunto un **Common Interface con le CAM estraibili, dove potete**

scegliere voi quale utilizzare Irdeto, ViAcces, Aston o la Cam Magic... (quest'ultima si può programmare per qualsiasi pro-



Il programmatore di schede Multipipo, che si usa con le schede Wafer Card.

vider, unica nota dolente è il prezzo 240 euro +il programmatore 20 euro). Naturalmente **le trasmissioni di Stream e Tele Più sono cifrate, e quindi visibili solamente dall'utente che sottoscrivere un abbonamento con l'emittente**. Dopo la sottoscrizione di questo, all'utente è consegnata una Smart Card. Questa contiene un chip, compito del chip è di comunicare con la CAM.

>> Protezione

Una volta che la Smart Card è inserita nel decoder, questo invia un reset alla card, la quale risponde l'**ATR (Answer To Reset)** con informazioni sul protocollo seriale usato (velocità, bit di start e di stop). La CAM poi richiede alla scheda di identificarsi con il serial number (ascii ed esadecimale) simile a questo:

```
Richiesta:
Cards ASCII Serial Number
    01 02 00 03 00 00 3F

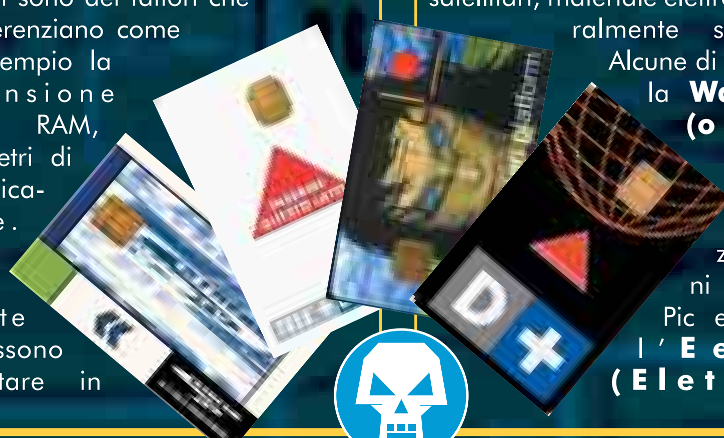
Risposta:
Cards ASCII Serial Number
    01 02 00 00 00 03 00 14
    3X 3X 3X 3X 3X 3X 3X 3X 3X
3X 44 35 36 30 34 31
    41 20
```

Vengono scambiate poi altre informazioni, riguardanti l'emittente e il paese. Poi la CAM invia la propria key (le chiavi di decodifica). Dopodiché la CAM invia un **ECM (Entitlement Control Message)** contenente due chiavi di decodifica del canale criptate, un identificativo del canale da decifrare (ch id) e il numero di chiave che la Smart card dovrà utilizzare. La Smart Card a questo punto controllerà se è abilitata alla visione del CH ID e se possiede la **key di decodifica (KN)** appropriata. In questo caso decifrerà la key e la rinvierà alla CAM ricriptandola con la CAMKEY. Dopo l'invio di un ECM, La CAM, ricevuta la key K1 dalla Smart Card, la decifrerà usando la CAMKEY in suo possesso e quindi sarà in grado di mettere in chiaro il canale. Se la smart non è abilitata alla visione del canale genererà come risposta un errore del tipo: **"Errore nella Key" o "Errore nel bouquet"**!

>> Sceglíete una carta...

Le Smart Card sono state progettate per vari usi, come per la memorizzazione d'informazioni (Come quelle che rilasciano le varie Università agli studenti).Il mondo del digitale è in continua evoluzione, si cerca di migliorare sempre e in ogni modo, vi sono tantissimo tipi di Card, che possono essere divise in più categorie: quelle di sola memoria, quelle con memoria logica di sicurezza e memoria con CPU. Tra le varie Smart Card vi sono dei fattori che le differenziano come per esempio la dimensione della RAM, parametri di comunicazione.

Queste si possono acquistare in qualsiasi negozio di apparecchiature satellitari, materiale elettronico e naturalmente su Internet. Alcune di queste sono: la **Wafer Card (o PicCard)** caratterizzata perché monta due zoccoli esterni uno per la Pic e l'altro per l'**Eeprom (Eletrically**



IL SIGNIFICATO DEI LED

Alcune di queste card hanno sette Led. I Led possono assumere significati diversi a seconda del software caricato sul processore stesso. In ogni caso i 7 Led sono suddivisi in 2 gruppi. Un primo gruppo di 3 Led generalmente composto di un Led rosso, uno giallo e uno verde, chiamati ControLed e in genere indicano: il rosso problemi di decriptazzione, il giallo superencrption in uso oppure assumere significati particolari, il verde che la card è occupata a rispondere ad un ECM. L'altro gruppo di quattro Led tutti dello stesso colore, giallo o verde generalmente, sono definiti keyleds e in genere indicano l'indice del provider in uso o della key in uso.

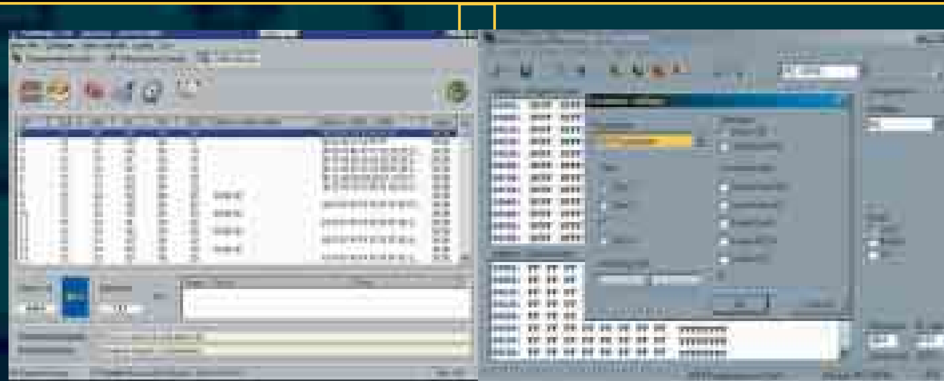


Una scheda PicCard2, con i suoi led di controllo.

Seca 2 è stato craccato!

Se in questo periodo con l'avvento del nuovo sistema Seca2 non solo vi siete trovati in difficoltà, ma avete anche fatto spese esagerate e/o inutili fate in modo che non ricapiti la prossima volta. In internet si trovano tante "bufale", falsi profeti che approfittano della buona fede delle persone!
In ogni caso, dopo mesi di bufale (schede autentiche ma a tempo spacciate come schede pirata senza scadenza...), qualcuno è riuscito davvero a craccare anche Seca2.
Il metodo si basa sull'accoppiamento tra una card originale e una FUN 4th generation opportunamente programmata. Con il solo abbonamento base, qualcuno è quindi riuscito ad "aprire" completamente il famoso Provider con tutto il pacchetto completo (Palco compreso!). Pare che anche con PicCard2 si sia risuciti a fare qualcosa di simile, anche se in modo più complesso. Si pensava che questo nuovo sistema avesse posto la parola fine al fenomeno della pirateria, almeno per un po' di tempo, ma... "Fatta la legge, trovato l'inganno".





La varietà di software per programmare le schede è davvero notevole.

Erasable Programmable Rom), la Gold Card e la Silver Card che sono esteticamente differenti dalla Wafer Card ma funzionano allo stesso.
La Fun Card (l'ultima uscita e la 5th) è un'alternativa alla PicCard, poiché con il suo microcontrollore AT90S8515 (o AT90S8515A) con 8K di memoria, 512 byte di SRAM e 512 byte d'Eeprom può ottenere risultati impensabili con le PicCard. Generalmente al processore è associata una memoria Eeprom esterna 24c64 o 24C65 per contenere i dati personali.
Poi vi sono le **PicCard2 che non hanno ancora la fama delle Fun, ma senz'altro sono almeno altrettanto interessanti per le loro potenzialità**. Questo tipo di card prevede l'utilizzo del PIC16F876 (28 pin) in combinazione con un'Eeprom 24LC16. Sono usate per emulare le altre Card originali. Per programmarle è necessario un Hardware specifico chiamato genericamente programmatore, ogni Smart Card deve essere programmata con il suo Programmatore, questo hardware va collegato con un cavo (anch'esso diverso secondo il programmatore) al PC che tramite un Software è in grado di interagire e quindi programmare la Smart Card.



Su Internet si possono trovare gli schemi per costruire card e programmatori. Questo è lo schema della FunCard.

>> I programmatori di schede

Vi sono quindi vari tipi di Programmatori. Si possono comprare facilmente su internet, dove si possono anche trovare anche gli **schemi di montaggio per chi si diletta a costruirli da se**.
Per programmare la Fun Card occorre il FunProg, collegato al PC tramite, un cavo seriale da 25 poli. Per la Wafer Card è necessario il Multipipo

Occhio a ciò che fate: si rischia grosso

Se attualmente la legge non punisce il singolo che cracca i sistemi di codifica satellitari, le forze dell'ordine sono particolarmente attente a chi diffonde chiavi di cifratura e vende schede pirata. I siti chiusi e i webmaster denunciati sono ormai numerosi, e difatti molti siti che riguardano questo argomento risiedono fuori dalla Unione Europea.

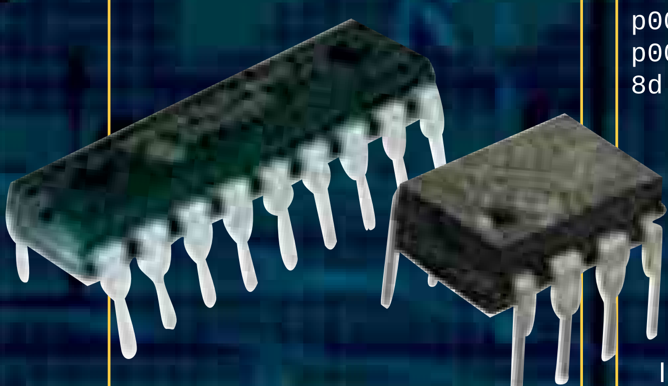


mentre per la Gold Card e la Silver Card va bene il Supermultipipo o Ludipipo (entrambi necessitano di un collegamento al PC tramite un cavo M/F 9poli). Sempre in Internet sono disponibili un infinità di Software che permettono di interagire con la Smart Card e l'apposito programmatore, prodotti da volenterosi programmatori. Tra i più conosciuti abbiamo:

IcProg: ideale per programmare le Pic e le Eeprom.

FunProm e Fun Magic: per le Fun Card.

Pic24c13: programma che gira sotto dos per programmare le Wafer Card con interfaccia Ludipipo.



Multiprog: utile sia per le Pic Card2 che per Le Fun Card.

CardWizard: sicuramente il miglior software per inviare comandi alle schede. È un programma velocissimo, stabile e ricco di funzionalità. La versione originale è in tedesco, ma fortunatamente è possibile reperire anche la Versione tradotta in italiano.

CardMaster: un buon software , un po' capriccioso perché per ogni minima cosa si blocca ma se è opportunamente settato funziona a meraviglia (ha qualche bug). Per questo sono disponibili versioni tradotte in italiano.

>> I codici

Per essere abilitati alla visione in chiaro dei canali, nella Smart Card devono essere memorizzate tre serie di dati:

1. Il Date Stamp. Ogni giorno un codice diverso che è una stringa di due byte è trasmesso alla carta . Es 02 31.

2. Un Channel ID valido. Un codice di due byte come, per esempio, FF FC o 00 05.

3. Una Key (chiave) valida. Questa è una stringa di nove byte in cui il primo byte rappresenta il Key idetificator, per esempio simile al il seguente:.

```
p00 direct   0443df   key
p00: 04: 05 c8 f3 69 1f a1
8d e4 <>
```

In ogni carta è memorizzato un **Provider ID** (tre byte, per esempio **04 43 df**) I primi due byte rappresentano il Provider Group mentre il byte finale identifica la carta specifica.

I "pirati" usano il programmatore con l'apposita Card per inserire il software per emulare le Card originali. Sulla Card pirata vengono caricati le Key, le chiavi di accesso, naturalmente diverse a seconda della Card in questione.

Per esempio, sulle Wafer sono caricati un file Hex per la Pic che emulano le Smart Card originali, mentre per l'Eeprom un file Bin,che contengono i codici operativi. Sulle Fun Card Viene caricato un file Flash, un file sull'Eeprom esterna e uno su quell'interna.

Le key sono composte da 8 byte più uno iniziale per identificare la key che sono, per ogni Provider:

02 - 04 - 06 - 08 - 0a - 0c - 0e - 10

In ogni card ci possono essere massimo 16 chiavi cioè otto per provider 00 e 8 per provider 10. Ogni canale per essere decodificato ha bisogno della giusta chiave per metterlo in chiaro altrimenti non si vede pur avendo inserito i chanid giusti. Come avete potuto notare sono ancora molti gli argomenti da trattare e approfondire, e cercheremo di farlo nei prossimi numeri.

LordAle

Sat Links

Spesso i siti che riguardano le codifiche satellitari vengono aperti e chiusi a un ritmo altissimo: a volte vengono rimossi per sempre; altre volte per poche ore (il tempo di mettere i nuovi codici e ultime notizie). Se trovate un errore tipo "pagina non trovata", non demordete, e provate in altri orari.

www.pesca2.da.ru
www.sistema-crakkato.da.ru
http://batmansat.tux.nu
www.europasat.da.ru
www.infoseca2.da.ru
www.scorpionsat.da.ru
www.pablo-sat.da.ru
www.vinhexsat.cjb.net
www.emosat.da.ru
www.capitanfabius.net
www.blacksat02.da.ru
www.presosat.da.ru
www.freeserversat.da.ru

Se poi volete acquistare Smart Card di ogni genere, programmatori e tante altre cose, uno dei siti più gettonati è www.chipplanet.it

COME FUNZIONANO I SISTEMI PER SCAMBIARE FILE, MUSICA E FILMATI



I Love 2 Peer

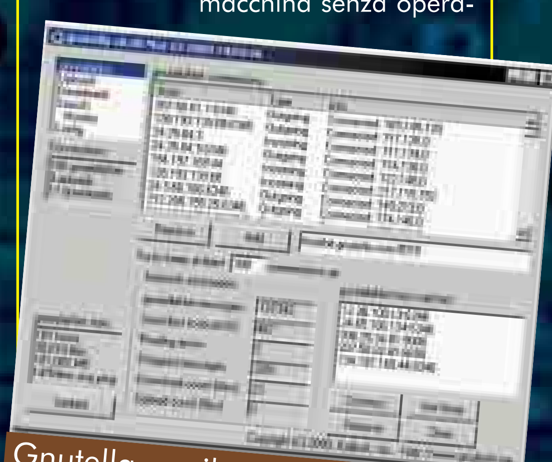
Come è strutturata la tecnologia, quali sono i campi d'impiego e gli scopi più o meno ufficiali e quali i fatti di cronaca di cui è stato protagonista.

Qualcuno ha definito l'avvento del Peer to Peer (più brevemente, P2P) **una vera e propria rivoluzione, paragonabile a quella dell'introduzione dei browser** a interfaccia grafica. In verità si tratta di un progetto a cui si lavora da anni, ma che solo l'avvento delle connessioni a banda larga (nonché la disponibilità di processori potenti e hard disk spaziosi a prezzi accettabili) ha potuto rendere attuabile nella pratica quotidiana. E se P2P non è una sigla che dica molto a tutti, provate invece a dire **Gnutella, Napster, KaZaa... o anche SETI@home**, perché, non dimentichiamolo, il P2P non è solo condivisione di file, ma anche di risorse hardware, ovvero spazio su disco e tempo processore.

>> Forse non tutti sanno cos'è

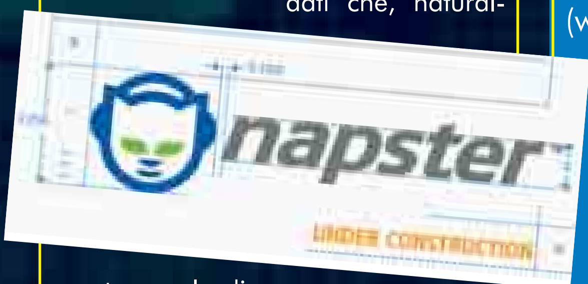
Si definisce P2P la condivisione di risorse informatiche attraverso lo scambio diretto, in alternativa alla tradizionale architettura client/server. Uno dei vantaggi è che, pur essendo una tecnologia relativamente nuova, **non richiede infrastrutture particolari, anzi, fa uso di quelle preesistenti, ottimizzandone l'utilizzo**.

Tanto per rendersi conto della differenza fra i due modelli, si pensi che, nel sistema client/server, il client, ovvero una macchina qualunque fra quelle connesse in rete, invia una richiesta al server, tipicamente una macchina senza opera-

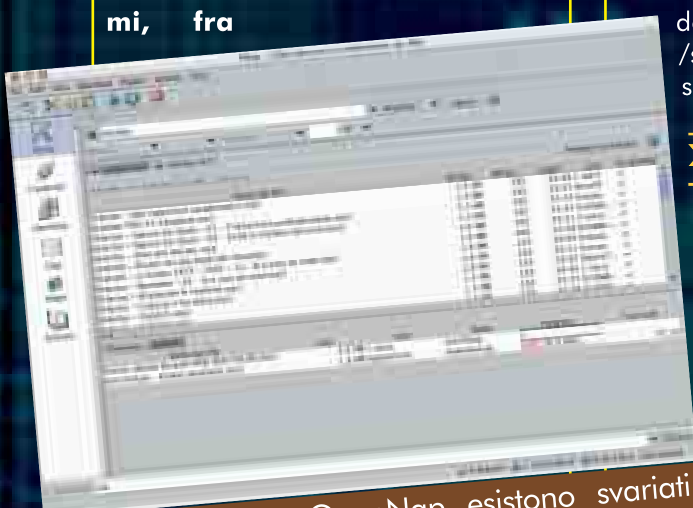


Gnutella a il vantaggio di non dipendere da un server centrale, ma i risultati delle ricerche sono molto variabili.

tore, dedicata a servire da riferimento per le richieste, che riceve la richiesta e la esaudisce. Invece, **nel peer to peer, ogni singola macchina connessa in rete è un peer, ovvero un partecipante che è al tempo stesso client e server nei confronti delle altre macchine della rete**. E questo vale sia per l'elaborazione dati che, naturalmente, per la distribuzione di file.



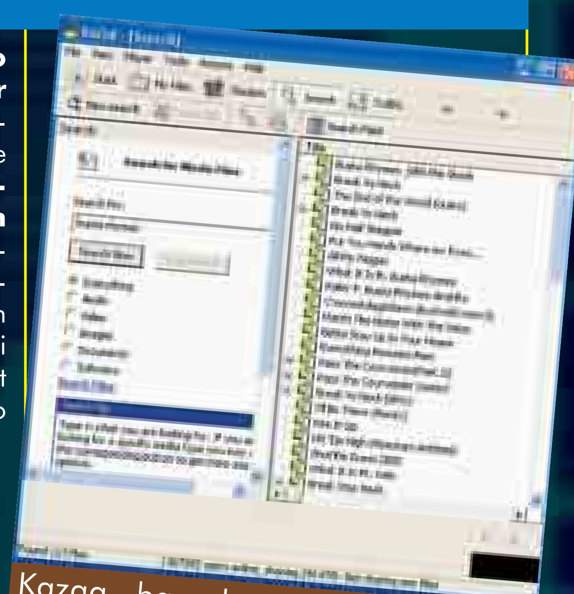
Per essere precisi, i sistemi di P2P utilizzano marginalmente anche il sistema client/server, soprattutto per quanto riguarda il file sharing: un server di riferimento (tipicamente, uno dei client connessi che accetta questo ruolo, un "supernode", come è chiamato in alcuni sistemi) mette a disposizione le proprie risorse hardware (tempo processore) e "dirige il traffico" verso i vari peer, gestendo l'elenco dei file condivisi e le richieste di ricerca, con relativa generazione degli elenchi di file corrispondenti ai criteri fra quelli presenti sui client connessi. **Alcuni sistemi, fra cui lo stesso Napster, facevano uso di un vero e proprio server centrale** per la gestione di tali processi, ma si è presto compreso che **questa modalità si rivelava essere più una debolezza che un vero punto di forza**: in caso di fermo del server, tutto il sistema diventava inutilizzabile, soffrendo così in fin dei conti degli stessi difetti del tradizionale sistema client /server che si sarebbe voluto superare.



Per il protocollo OpenNap esistono svariati client per tutte le piattaforme, e centinaia di server distribuiti. Questo è XNap, un client scritto in Java che esiste per Windows, Linux e Mac OS.

>> Come funziona

A questo punto il meccanismo è chiaro: **un utente entra in rete effettuando il login al circuito P2P, e diventa peer, mettendo a disposizione le proprie risorse a tutti gli altri**; può quindi inviare le sue richieste agli altri peer, e contemporaneamente resta a disposizione per accogliere le richieste altrui. Ogni macchina, nel doppio ruolo di server e client (qualcuno chiama questa ibridizzazione "servent") **gestisce richieste in entrata e in uscita, passando i dati in relazione al relativo TTL** (Time To Live, in parole povere la "vicinanza" di due macchine in rete nei passaggi da una all'al-



Kazaa ha alcune caratteristiche molto interessanti, ma è un protocollo proprietario e non sfruttabile con tutti i sistemi.

Non solo Mp3

Il P2P non è solo caccia ai marziani o all'ultimo successo pop: molte aziende hanno adottato questo sistema a livello professionale, preferendolo, per i motivi già menzionati, al tradizionale client/server, sia per gli utilizzi aziendali classici (condivisione di file e lavoro collaborativo in rete) che nel nuovo territorio di frontiera dell'e-commerce.
A titolo di cronaca si nominano qui IM-Live (www.hotcomm.com/IMLive.asp), sistema di messaggistica dedicato all'e-commerce, che sfrutta il P2P per stabilire un contatto diretto fra gli interlocutori, potendo quindi contare su una maggior sicurezza e PruneBaby (www.prunebaby.com), una vera e propria rete di vendita e acquisto in P2P, una specie di "mercatino globale".
Vanno inoltre menzionati i sistemi di condivisione risorse, sul modello di SETI@home, uno dei quali è Entropia (www.entropia.com), che organizzano l'utilizzo dei cicli idle di tutte le macchine connesse in rete per effettuare calcoli di grande complessità, spesso volti anche a nobili scopi, quali la ricerca sul cancro o altri progetti medici e scientifici.

I PRINCIPALI SISTEMI DI SCAMBIO

Gnutella
www.gnutella.org
La sua particolarità è quella di non aver bisogno di un server centrale, ed è quindi impossibile da censurare completamente. Il protocollo è libero, per cui chiunque può realizzare programmi. Su Windows i client più famosi sono BearShare (www.bearshare.it) e LimeWire (www.limewire. com), che è un programma in Java che funziona anche sotto Mac OS (clasic e X) e Linux.

Kazaa
www.kazaa.com
È un sistema proprietario, ma che ha alcune interessanti caratteristiche, prima tra tutte quella di assegnare una sorta di "punteggio" ai migliori utenti (quelli che condividono molti file e per molte ore al giorno). Questo "punteggio" permetterà di superare nelle code di dowload gli utenti che non condividono, o che usano poco il sistema. Il client ufficiale esiste solo per WIndows; per Mac e Linux esistono programmi che si appoggiano alla rete di Kazaa, ma non offrono le stesse funzionalità.

OpenNap: Open Source Napster

OpenNap
http://opennap.sourceforge.net
Basato sul vecchio protocollo di Napster, OpenNap ha il vantaggio di essere completamente open source e di consentire quindi a chiunque di creare il proprio server per accentrare le funzioni di ricerca. Sono quindi nati centinaia e centinaia di server, alcuni specializzati su un certo tipo di file (audio, video, software, documenti…) o per genere musicale (rock, etnica, classica…). I client più popolari sono WinMx (che vedremo anche in seguito) e XNap (http://xnap.sourceforge.net), che essendo scritto in Java esiste anche in versioni Linux e Mac OS X.

WinMx
www.winmx.com
Oltre a poter funzionare anche come programma OpenNap, WinMx ha anche un suo protocollo proprietario, che ottimizza alcune funzionalità, come la possibilità di scaricare da più utenti contemporaneamente o di cercare automaticamente fonti alternative per il download.

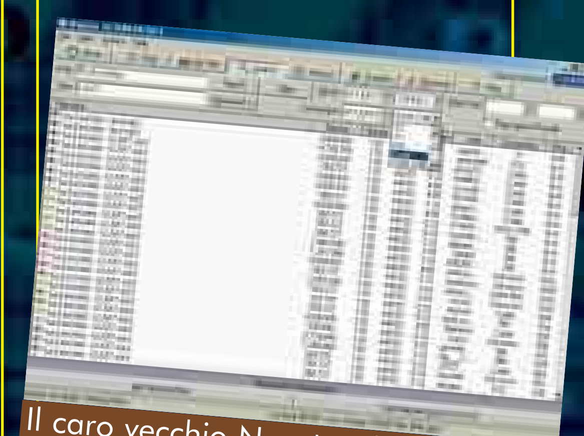
Freenet
www.freenetproject.org
Freenet è stato pensato per impedire qualsiasi tipo di controllo e censura sui contenuti scambiati, ed è quindi basato su sofisticati sistemi di anonimato e crittografia, oltre a essere completamente decentrato. Il tutto è molto interessante, ma al momento non è così semplice installare e configurare adeguatamente i programmi necessari. Vale comunque la pena di provarlo e tenerlo d'occhio.

tra). Per fare un esempio pratico, la macchina A entra in rete e comunica la propria presenza e le proprie istanze alla macchina B, e la macchina B fa la stessa cosa con i propri dati e con quelli della macchina A alla macchina C… e così via. Ma si arriverà ad un punto in cui, poniamo, la macchina M si rifiuterà di prendere atto delle istanze della macchina A, non accettando comunque di comunicare con essa per via dei troppi passaggi necessari per raggiungerla. Ovviamente, trattandosi di una rete multidimensionale e non lineare, le interconnessioni sono tanti e tali che il problema è solitamente del tutto marginale.

Naturalmente parliamo di richieste a livello di ricerca: **una volta stabilita la connessione fra le due macchine, a prescindere dal loro TTL, lo scaricamento avviene direttamente**, in P2P, appunto.

Risulta evidente che non c'è alcun bisogno di server — intesi come luoghi fisici in cui i file vengono depositati, o ai quali si deve accedere per utilizzarne le risorse - ed è questa la vera rivoluzione: **nessun vincolo, nessuno dei limiti noti per i sistemi centralizzati… e ben poco controllo**.

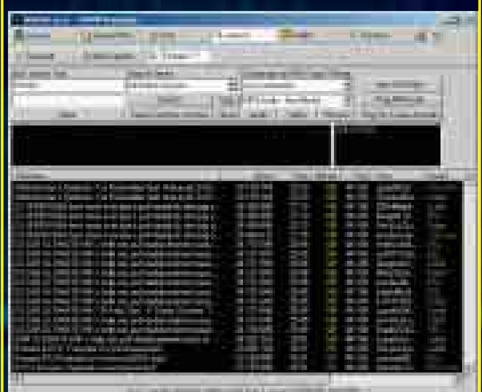
Ma la rivoluzione è anche culturale: **non esiste più il popolo dei leechers, sterili scaricatori anonimi di file, ma una vera e propria comunità**, all'interno della quale si possono stabilire relazioni di vario tipo, che vanno dal semplice "non staccare finché non ho finito di scaricare, per favore" o "se ti passo X, mi metti avanti nella coda per scaricare Y"? fino ad arrivare a veri e propri **gruppi di interesse, che collaborano per raccogliere materiale su un determinato argomento per metterlo a disposizione di tutti**, o che accettano di buon grado di fornire spazio e risorse a una causa, buona o frivola che sia. Una rete non più di macchine, ma di persone. E non è cosa da poco.



Il caro vecchio Napster, il primo sistema P2P a guadagnarsi una fama mondiale.

>> La breve (ma intensa) storia del P2P

Il P2P, ai suoi albori, comincia gradualmente ad affermarsi come supporto ai programmi di ricerca collettiva. Il già citato SETI@home, il più popolare nel genere, si propone infatti di **utilizzare il tempo processore "morto" delle macchine connesse alla sua rete** (quando la macchina è connessa ma non sta svolgendo compiti che la impegnino in particolar modo) **per effettuare ricerche sulla presenza di vita nello spazio**. Ma è con l'affermazione dell'algoritmo Mp3 che il P2P conosce la sua vera popolarità: la possibilità di alleggerire i file audio e video, prima di allora notevolmente ingombranti, a tal punto da poterli agevolmente trasportare su vari tipi di supporto, nonché distribuirli in Rete, è vista come un vero e proprio miracolo.



Oltre a lavorare con il suo protocollo proprietario, WinMX può collegarsi anche ai server OpenNap, cosa che lo rende molto più versatile di altri concorrenti.

Come è immaginabile, a questo punto il P2P si tramuta da fatina buona, dispensatrice di risorse per nobili scopi, a **orribile demone iconoclasta, che si fa beffa di royalty e diritti d'autore e che trascinerà alla rovina il mercato discografico e cinematografico** (scaricando misteriosamente di ogni colpa l'aumento vertiginoso dei costo dei supporti). Ben presto la mannaia della giustizia, impugnata da editori e autori, cala sui client, senza però fermarli. Il miracolo è compiuto, e non si torna indietro: la peculiare struttura della rete P2P rende impossibile bloccarla o monitorarla in alcun modo. E a nulla valgono molto neppure gli espedienti di protezione, come impedire la copia di un supporto o legare l'edizione elettronica di un brano musicale a una determinata macchina o dispositivo di riproduzione: si tratta di iniziative goffe e inutili, che oltre a creare problemi agli utenti standard non limitano in alcun modo la diffusione "clandestina". E da qui è cronaca. **Napster è la prima e per ora unica vittima della lunga mano della giustizia**, vuoi per scelte discutibili da parte del suo fondatore, vuoi per generale impreparazione nei confronti del fenomeno e dei relativi attacchi ad esso mossi. AudioGalaxy esiste ancora, ma è pesantemente storpiato da un meccanismo di filtri che –in pratica– fa sì che non sia possibile ricercare nessun contenuto protetto da copyright. Ma i suoi successori hanno avuto spalle più larghe, e a tutt'oggi, nonostante le numerose iniziative legali intraprese dai soggetti che vedono nel P2P una minaccia al diritto d'autore, **KaZaa, WinMX e soci godono di ottima salute**. E molti autori sono scesi in campo fra le fila della causa del file sharing, sostenendo che si debbano abbandonare i vecchi modelli di distribuzione e che il P2P è un fenomeno fondamentalmente irrefrenabile e soprattutto utilissimo per la diffusione capillare dei prodotti dell'ingegno.
Come dicevamo all'inizio, questa è solo un'introduzione all'argomento: nei prossimi numeri esamineremo i vari sistemi di scambio file, vedendo per ciascuno quali sono i trucchi per trovare quello che si cerca e scaricarlo nel minore tempo possibile.

Paola Tigrino

Il gergo del Peer to Peer

Sharare: Condividere i propri file con gli altri utenti del network.

Trade, Trader: I Trader sono quegli utenti che condividono i propri file, ma solo con persone che possiedono una adeguata "merce di scambio" (io ti do quello che cerchi, se tu puoi darmi ciò che mi interessa). Non sono molto ben visti dalla comunità.

Leecher: Chi si collega a un network P2P per scaricare file dagli altri, ma senza condividere nessuno dei propri file. Molte persone annullano il download di un altro utente se si accorgono che questi è un leecher.

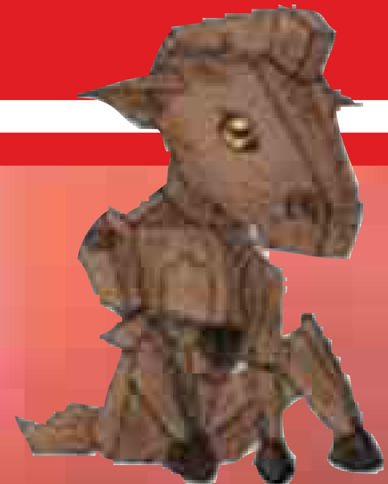
Screener: Copia illegale di un film ottenuta da videocassette o DVD distribuite in anteprima ai critici, ai giornalisti o ai distributori cinematografici. Gli screener sono molto ambìti, perché costituiscono delle anteprime ma la copia è generalmente di buona qualità (meglio delle copie fatte con la videocamera).

Telesync: Copia illegale di un film ottenuta filmando lo schermo di un cinema durante la proiezione, ma collegando l'uscita audio al sistema di amplificazione del cinema. Il sonoro è buono, ma il video è di bassa qualità.

Cam: Copia ottenuta filmando direttamente lo schermo di un cinema durante la proiezione. Sono le copie con la peggiore qualità in assoluto.

DVD-Rip: Copia di un film ottenuta convertendo un DVD commerciale. La qualità è la migliore in assoluto, ma queste copie arrivano sui network P2P solo molti mesi dopo l'uscita nelle sale, quando appunto viene prodotto il DVD commerciale.

UN UTILE PROGRAMMA PER RIMUOVERE I CAVALLI DI TROIA



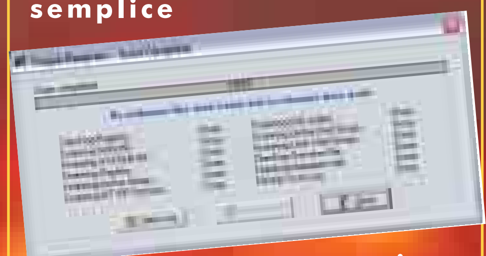
Un'arma contro la cavalleria trojana

Volete verificare se sul vostro sistema è presente un Trojan, oppure non riuscite a eliminare completamente uno che avete già rilevato? Trojan Remover potrebbe essere il programma che fa al caso vostro.

Molto spesso viene usato impropriamente il termine "virus" per definire qualunque tipo di codice o programma che possa risultare dannoso.
Ve ne sono però alcuni, come i cosiddetti cavalli di Troia (chiamati in inglese Trojans), che nulla hanno a che fare con i virus veri e propri, trattandosi in realtà di programmi, mascherati da applicativi innocui (giochi, utility, screen saver, ecc…), **in grado comunque di causare danni anche gravi**.
La maggior parte degli antivirus moderni hanno la possibilità di riconoscere i cavalli di Troia più noti, ma **solo pochi sono in grado di eliminare completamente le tracce da un sistema colpito da questi fastidiosi programmi**.
Esistono tuttavia anche utilità di sistema specifiche, chiamate in gergo "antitrojan", progettate con lo scopo di intercettare, localizzare e rimuovere applicazioni come i cavalli di Troia, sfruttando un enorme database aggiornabile via Internet, analizzando i file di sistema, registro compreso, e controllando i processi attivi.

>> Perché i Trojan?

Tutto questo poiché vi è una notevole gamma di attacchi possibili contro una macchina Windows. Del resto la crescita esponenziale delle righe di codice nei sistemi operativi, o nei programmi in genere, provoca un conseguente aumento nel numero di "falle" sfruttabili per attacchi di ogni tipo.
L'intento comunque in questi casi è sempre quello di poter accedere alle risorse del sistema senza che il legittimo utente od amministratore se ne accorga.
A questo proposito **l'opzione più semplice consiste nell'installare nella macchina un programma capace di garantire un accesso completo, aprendo vie di comunicazione che sfruttano librerie di sistema** destinate alla comunicazione tcp/ip (le cosiddette "winsocket").

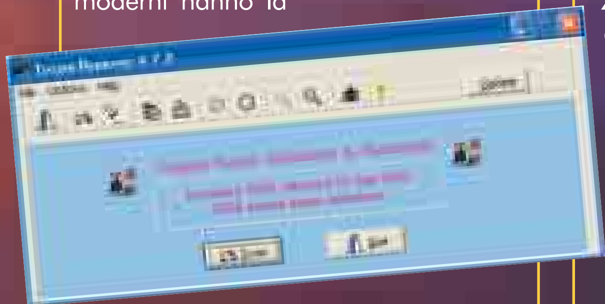


Ogni linguaggio può essere utilizzato per creare una piccola architettura client-server.
Non a caso quasi giornalmente vengono sviluppati programmi di questo genere sia in Delphi che in Visual Basic - ma anche nel più complesso C/C++ - tanto da essere considerati ormai solo degli esercizi di stile.
In questi casi **non è sufficiente aggiornare frequentemente il database del proprio antivirus**: i troiani prolificano molto più velocemente dei virus e dunque c'è sempre un buon margine di probabilità che il nostro sistema vanga infettato da un software non riconosciuto correttamente.
A riprova di quanto detto si pensi che di tali programmi sono disponibili i sorgenti in vari linguaggi: è dunque molto facile per un programmatore studiare il codice e "creare" nuovi troiani secondo le proprie esigenze.

>> Trojan Remover

Tra i molti programmi che possono aiutare a difenderci da questi pericoli vi è "Trojan Remover", un pratico programma che esegue non solo la scansione del disco rigido ma anche quella di tutto il sistema in genere.
TR può essere scaricato gratuitamente, tra i tanti altri, dal sito della casa software che l' ha prodotto, ovvero la Simply Super Software, raggiungibile all'indirizzo www.simplysup.com/tremover.
Le piattaforme per cui TR è stato sviluppato sono quelle della famiglia Windows 9.x/Me/NT e XP, sebbene sia stato usato con efficacia anche in ambiente Win2000.
Appena terminata la consueta procedura d'installazione si può avviare il programma: apparirà quindi un'interfaccia d'ingresso che ci chiederà se vogliamo registrarci per acquistare il prodotto.
È importante notare che TR non richiede nessuna impostazione particolare per poter funzionare in modo corretto e completo.
Le operazioni che TR è in grado di compiere spaziano dalla **scansione dei file di registro fino all'analisi dei file e dei programmi che vengono caricati ogni volta che si accende il computer**.
Ogni volta che TR individuerà un trojan horse o un programma non identifica-

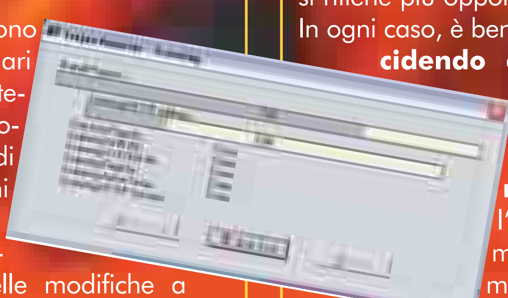
to, apparirà una finestra di pop-up che mostra locazione e nome del file.
A questo punto verrà offerta la possibilità di **rimuovere l'oggetto in questione dai file di sistema e di rinominarlo**, in modo che non possa essere più caricato.
Purtroppo infatti molti cavalli di troia moderni hanno la



capacita di attivarsi alla partenza di Windows rendendo inoltre difficoltosa anche la loro rinominazione.
Di conseguenza **TR può ravviare il sistema e rinominare i file dannosi prima che Windows entri in funzione**. Scegliendo questa opzione tutti i file di sistema vengono impostati in "sola lettura", prevenendo quindi una nuova infezione.
Al termine delle procedure di avvio i parametri di "sola lettura" vengono quindi rimossi.

>> Prima scansione

La scansione del sistema può essere facilmente iniziata dall'interfaccia principale tramite l'apposito pulsante. La prima volta che si effettuerà questa operazione, TR chiederà di selezionare le estensioni dei file che si vogliono analizzare, "ricordando" la vostra risposta per le scansioni future.
In ogni caso non sono necessarie particolari conoscenze in materia, in quanto il programma offre già di default delle opzioni più che sufficienti.



Se in futuro si volessero apportare delle modifiche a queste impostazioni basterà, fare clic sul pulsante "Options" dalla finestra "Drive/Directory Scan", che porta alla sezione dedicata alle preferenze sui tipi di file da analizzare.
La scansione può essere interrotta in qualsiasi momento, impedendo a TR di compiere qualsiasi azione correttiva su eventuali file trovati infetti; lasciandola invece terminare correttamente, sarà poi possibile visualizzare i file di log con una specie di sommario sulle operazione compiute.

>> Scansioni di tipo particolare

La barra delle applicazioni dell'interfaccia principale mette inoltre a disposizione, tramite il pulsante identificato con la torcetta, la possibilità di compiere altri tipi di scansioni.
Queste possono essere la **scansione di singole cartelle o di interi drive**, selezionati partendo dalla solita finestra "Drive/Directory Scan", che mostra inoltre un menu per scegliere il tipo di operazione che TR effettuerà nel caso dovesse riscontrare la presenza di un cavallo di troia.
Le opzioni possibili sono la **rinominazione automatica del file infetto** (a meno che questi non si trovi dentro un archivio zippato, nel qual caso si richiede l'intervento dell'utente), **oppure la semplice annotazione nel file di log del resoconto della scansione**.
È prevista inoltre anche la messa in pausa a ogni file contenente un trojan, o sospetto tale, per permettere di prendere, di volta in volta, la decisione che si ritiene più opportuna.
In ogni caso, è bene ricordare che **decidendo di eliminare un file con Trojan Remover si compie un'azione irreversibile**, poiché l'oggetto verrà rimosso senza nemmeno essere spostato prima nel cestino.
Una funzione molto pratica e comoda viene dalla possibilità di compiere gli stessi tipi di scansione direttamente da Windows Explorer, premendo semplicemente, una volta selezionato il file o la cartella, il tasto destro del mouse.



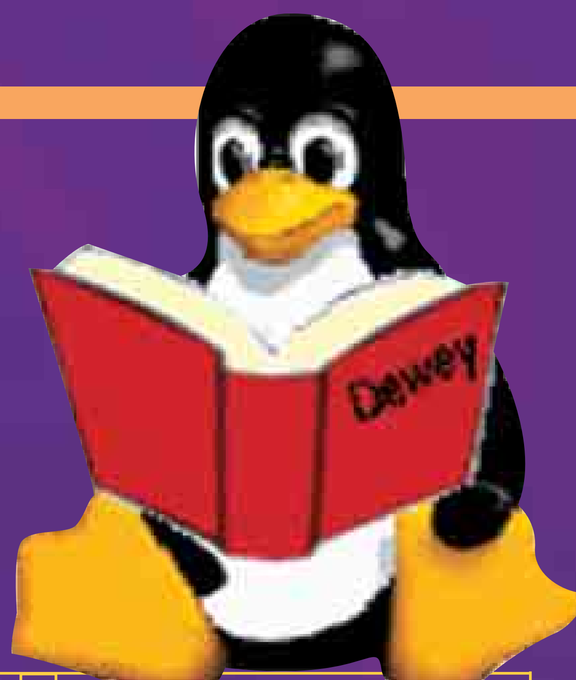
Se durante il funzionamento di TR doveste notare la creazione di cartelle nella directory dei file temporanei di Windows (C:\Windows\Temp\) non dovete preoccuparvi, poiché è del tutto normale. Queste cartelle verranno rimosse automaticamente in breve tempo. Le altre funzioni dell'interfaccia principale permettono un accesso rapido ai file di log e alla loro stampa, l'abilitazione allo scan d'avvio di cui abbiamo parlato prima e per finire alla visualizzazione del database dei trojan conosciuti.

Fabio Mingotto

PREZZO E PAGAMENTO

La registrazione di Trojan Remover costa circa 25 dollari, ma il fatto di non pagare non preclude il funzionamento dell'antitrojan. Passati alcuni secondi infatti, il pulsante "Continue" diverrà attivo, consentendo di accedere all'interfaccia principale.Se però il programma vi è stato utile, dare un giusto compenso ai programmatori è il minimo che si possa fare. Magari mettendosi insieme a qualche amico e facendo un acquisto di gruppo.
L'azienda offre la possibilità di effettuare il pagamento dal suo sito, oppure fornendo i dati richiesti tramite fax o direttamente per telefono.

COME ORIENTARSI TRA LE VARIE VERSIONI DEL KERNEL



LINUX: diamo i numeri

Grazie al contributo di una popolosa comunità di sviluppatori, il Kernel di Linux viene continuamente migliorato e aggiornato: come si fa quindi a distinguere le varie versioni?

Inizialmente ogni versione di Linux che veniva rilasciata era identificata da un numero progressivo: 0.01, 0.02, 0.95 e così via... Tuttavia si comprese ben presto che tale tipo di numerazione era inadeguata e, a partire dalla versione 1.0, il sistema di numerazione del kernel Linux venne modificato, permettendo di organizzare in maniera efficace lo sviluppo. Da allora ogni versione del kernel è identificata da tre numeri, ciascuno con un preciso significato. Il primo è il cosiddetto numero principale della versione; questi viene modificato solo nel caso in cui le modifiche al kernel siano veramente notevoli, al punto che il passaggio da un 'major number' a un altro può essere considerato un evento storico! Per quanto riguarda il secondo numero, che indica invece la serie del kernel, le cose si complicano leggermente. Lo sviluppo di Linux segue contemporaneamente binari differenti: mentre una parte degli sviluppatori è ad esempio impegnata a lavorare ad una nuova versione, eliminanodone bug e rendendola così il più possibile affidabile, altri programmatori e testers stanno già lavorando a pieno ritmo alla nuova serie del kernel. Si è stabilito che per convenzione i kernel della serie 'stabile' hanno un numero pari: di solito lo sviluppo di questa serie consiste principalmente nella correzione dei bug e nell'aggiunta delle componenti strettamente necessarie e, vista la loro comprovata stabilità, quasi tutte le distribuzioni sono basate su kernel appartenenti a questo ramo di sviluppo. Numeri dispari sono invece assegnari alle serie 'instabili', dove i kernel contengono codice meno testato, funzionalità sperimentali o innovativi algoritmi. Nuove versioni dei kernel appartenenti alla serie instabile vengono rilasciate con grande frequenza e, per chi volesse provarli, il consiglio è quello di avere una macchina dedicata appositamente per questo scopo onde evitare spiacevoli inconvenienti. Infine ad ogni nuova release è associato anche un numero progressivo; in base alla quantità e all'importanza delle modifiche apportate, tra il rilascio di una versione e la successiva possono trascorrere pochi giorni o persino settimane.



>> Qualche esempio...

Il passaggio dalla versione 1 alla versione 2 del kernel Linux, avvenuta sei anni e mezzo or sono, portò con sé radicali cambiamenti; in particolare, come abbiamo già visto qualche numero fa, vennero introdotti i moduli del kernel a caricamento dinamico e il supporto per macchine multiprocessore.
Da allora tre serie stabili si sono alternate sui computer di migliaia di utenti: 2.0, 2.2 e 2.4; per quanto riguarda poi il kernel 2.4 in particolare, sono state ben 21 le diverse release che in un biennio si sono succedute. Per chiarire ulteriormente, vi basti pensare che il passaggio dalla serie 2.2 alla 2.4 ha introdotto sostanziali novità tra cui il supporto per USB, Firewire, Bluetooth e ReiserFS; al contrario, il kernel 2.4.19 ha "solamente" corretto numerosi bug della release precedente (la 2.4.18) e migliorato il supporto per alcune componenti hardware. Occore inoltre aggiungere che, mentre continua il lavoro

LINUX LINKS

www.kernel.org
Archivio ufficiale dei sorgenti del kernel Linux.

www.kernelnewbies.org
Per chi desidera conoscere più a fondo il kernel Linux e contribuire al suo sviluppo...

www.kernelhacking.org
La lettura del noto kernelhacking-HOWTO è sicuramente un ottimo punto di inizio!

www.tldp.org/LDP/tlk
Sebbene sia un po' datato, "The Linux Kernel" rimane ancora oggi un classico.



di rifinitura al kernel 2.4, già in molti (tra cui lo stesso Linus Torvalds) sono attualmente impegnati nello sviluppo di Linux 2.5; proprio da questa, che è una serie 'instabile', verrà un giorno alla luce il futuro kernel 2.6!

>> Le cose si complicano

Tra una release e l'altra, sia per i kernel della serie stabile che per quelli 'unstable', vengono rese disponibili numerose revisioni "di transizione" contenenti un ristretto numero di modifiche da testare; queste pre-release vengono indicate con il suffisso -preXX, dove XX è un numero che aumenta di volta in volta. Quando poi si ritiene che i tempi stiano divenendo maturi per il rilascio di una nuova versione, il -pre viene sostituito dalla sigla -rc, ovvero Release Candidate. Esistono inoltre varie patch temporanee rilasciate da diversi kernel hacker; molto spesso queste introducono alcune migliorie non ancora sufficientemente testate per poter essere inserite nel kernel ufficiale. In questo caso il nome della patch consiste nella versione di Linux con l'aggiunta di -XXYY, dove YY è sempre un numero incrementale e XX le iniziali dell'autore: comuni sono le patch -ac di Alan Cox e -dj di Dave Jones (un po' i factotum della situazione) così come da ricordare sono i miglioramenti apportati alla gestione della memoria virtuale grazie ai kernel targati -aa, ovvero del italiano Andrea Arcangeli.
Esistono infine alcuni kernel segnati con l'estensione -dontuse: questo significa che troppo tardi ci si è accorti dei gravi problemi che affliggevano la release in questione. Inutile forse dire che, nel malaugurato caso in cui fosse proprio il kernel da voi installato, è consigliabile effettuare un aggiornamento quanto prima.

>> A ciascuno il suo

Il gran numero di componenti del kernel Linux e l'altissimo numero di periferiche supportate ha spinto gli sviluppatori a formare diversi gruppi di lavoro i cui sforzi sono concentrati verso uno scopo ben preciso e circoscritto; la modularità di Linux ha favorito ovviamente questo, permettendo ai kernel hacker di lavorare indipendentemente ad un modulo piuttosto che a un altro.
In particolare, alcuni sviluppatori sono emersi tra gli altri per le proprie competenze e sono così divenuti, in maniera più o meno ufficiale, i maintainer cioè le persone responsabili di quella porzione di codice (ed è a loro che lo stesso Torvalds fa riferimento per eventuali problemi riscontrati con quella funzionalità). Greg KH è ad esempio il maintainer del modulo per il supporto delle periferiche USB e PCI Hotplug, Trond Myklebust è invece il responsabile del codice per il client NFS; il supporto delle partizioni NTFS è gestito invece da Anton Alta mentre maintainer del sistema Bluetooth è Maksim Krasnyanskiy e così via...



Inoltre esistono alcuni personaggi a cui è affidato il compito di gestire lo sviluppo generale del kernel; a loro spetta ad esempio l'ultima parola circa l'inserimento o meno di una funzionalità nel ramo di sviluppo ufficiale e sono sempre loro a stabilire quando rilasciare una nuova versione. Kernel Maintainer della serie stabile 2.0 è David Weinehall mentre è Alan Cox a gestire l'inossidabile serie 2.2; inoltre, mentre Linus Torvalds è personalmente impegnato nello sviluppo del nuovo kernel 2.5, Marcelo Tosatti prosegue nel suo lavoro di maintainer dell'attuale serie stabile 2.4. In particolare i kernel maintainer, prima di rilasciare nuove versioni per il grande pubblico, annunciano spesso dei freeze del codice; in pratica il sorgente viene "congelato" e non vengono più implementate nuove funzionalità bensì ci si limita ad individuare e correggere i bug presenti.
Come dire: per fare un grande kernel, ci vuole una grande organizzazione!

Lele altos.tk

Informazioni, alla vecchia maniera

Finger è un protocollo estremamente semplice e il cui funzionamento è dettagliatamente descritto nella RFC 742, scritta 25 anni fa! Sviluppato al MIT, finger è stato molto utilizzato in passato per ricercare informazioni sulle persone, e ancora oggi viene utilizzato in diverse applicazioni. Una delle caratteristiche principali di questo protocollo è la sua estrema semplicità; essenzialmente il client invia la richiesta spedendo una sola riga di testo e il server risponde inviando una risposta (che varia ovviamente in base alla richiesta) e chiudendo quindi la connessione (la comunicazione utilizza il protocollo TCP e avviene tramite la porta 79).
Gli sviluppatori Linux hanno implementato un server finger modificato ad hoc in grado di restituire un resoconto sullo stato dello sviluppo del kernel; digitando quindi da shell

```
finger linux@finger.kernel.org
```

potrete sapere immediatamente quali siano le ultime versioni rilasciate.

IDENTIFICATION ORDER NO.17
16 Gennaio 2003

WANTED

DIVISION OF INVESTIGATION
H.J. DEPARTMENT OF NET
CERNUSCO S.N., MI

Fingerprint Classification

16 0 5 U 001 20
I 17 U 001

SIRCAM

KIDNAPING

Alias: W32/SirCam@mm, Backdoor.SirCam, I-Worm.Sircam.a, WORM_SIRCAM.A, W32/Sircam-A, W32/Sircam, Win32.Sircam.137216, W32/Sircam.worm@mm, Win32.HLLW.SirCam

Sistemi a rischio: Windows 95, Windows 98, Windows Me

Sistemi immuni: Windows 3.x, Windows NT, Windows 2000, Windows XP, Macintosh, Unix, Linux

Il worm che trattiamo in questo numero è Sircam che, pur essendo quasi del tutto innocuo al momento, ha causato non pochi problemi in tutto il mondo qualche tempo fa e che potrebbe crearne tuttora a chi è sprovvisto di un antivirus. La particolarità di Sircam è che, per un bug contenuto nel proprio codice, è incapace di replicarsi sotto Windows NT, 2000 e XP. La diffusione è ormai limitata dato che tutti hanno un software di protezione al giorno dopo così la Symantec ha abbassato la soglia di pericolosità da 4 a 3.

Modalità di diffusione

Sircam si diffonde in svariati modi ma prevalentemente tramite E-Mail, il modo più semplice per colpire gli utenti meno esperti o protetti. L'infezione arriva come allegato a un messaggio E-Mail dalle seguenti caratteristiche:



Soggetto: Potrebbe essere casuale e sarà lo stesso uguale al nome dell'allegato.

Allegato: Sarà un file preso dal computer del mittente e avrà un'estensione bat, com, lnk o pif aggiunta a quella del file originale.

Messaggio: Il corpo del messaggio sarà casuale ma conterrà sempre una delle seguenti frasi a seconda della versione di Sircam.

Versione Spagnola

Prima riga:
`Hola como estas ?`
Testo centrale:
a) `Te mando este archivo para que me des tu punto de vista`
b) `Espero me puedas ayudar con el archivo que te mando`
c) `Espero te guste este archivo que te mando`
d) `Este es el archivo con la información que me pediste`
Ultima riga:
`Nos vemos pronto, gracias.`

Versione inglese:

Prima riga:
Hi! How are you?
Testo centrale:
a) `I send you this file in order to have your advice`
b) `I hope you can help me with this file that I send`
c) `I hope you like the file that I send you`
d) `This is the file with the information that you ask for`
Ultima riga:
`See you later. Thanks`

Dettagli tecnici

Quando il worm viene eseguito su un computer provvede subito a compiere le seguenti operazioni:

1. Crea nella cartella TEMP e in altre del sistema alcune copie di se stesso, contenenti l'infezione allegata a un altro file trovato nel computer. Questo documento contenente l'infezione viene poi eseguito usando il programma registrato per aprire quello specifico formato di file. Per esempio, se viene salvato come un file dall'estensione doc verrà eseguito usando Microsoft Word o Wordpad. Un file con l'estensione xls sarà aperto con Excel e uno con estensione zip con WinZip.

2. Copia se stesso nel file con nome C:\Recycled\Sirc32.exe e anche in C:\Windows\System\Scam32.exe.

3. Aggiunge il valore
`Driver32=%System%\scam32.exe`
alla chiave di registro
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices`

4. Crea la chiave di registro
`HKEY_LOCAL_MACHINE\Software\SirCam` con i seguenti valori:

`FB1B` Fornisce il nome del file contenente il worm nella cartella Recycled
`FB1BA` Fornisce l'indirizzo IP SMTP
`FB1BB` Fornisce l'email del mittente
`FC0` Fornisce il numero di volte che il worm è stato eseguito
`FC1` Fornisce qual'è il numero della versione del worm
`FD1` Fornisce il nome del file del worm che è stato eseguito senza l'estensione
`FD3` Fornisce un valore corrispondente allo stato attuale del worm
`FD7` Fornisce il numero di email che sono state inviate prima il processo fosse interrotto

5. Il valore (Default) della chiave di registro `HKEY_CLASSES_ROOT\exefile\shell\open\command` viene impostato a `C:\recycled\sirc32.exe "%1" %*`. Questo consente al worm di eseguirli ogni volta che un file exe viene avviato.

6. Il worm è network attivo ed elenca tutte le risorse network per infettare i file in condivisione. Se il worm trova uno di questi file:
• Copia sè stesso come Sirc32.exe
• Aggiunge la stringa
`"@win \recycled\sirc32.exe"`
al file di sistema Autoexec.bat
• Copia il file `Rundll32.exe` in `C:\Windows\Run32.exe`
• Sostituisce il file `C:\Windows\rundll32.exe` con `Sirc32.exe` creato in precedenza

7. C'è una possibilità su 33 che il worm esegua queste due operazioni:
• Copiare se stesso da `C:\Recycled\Sirc32.exe` a `C:\Windows\Scmx32.exe`
• Copiare sè stesso come "Microsoft Internet Office.exe" nella cartella indicata nella chiave di registro `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup`

8. C'è una possibilità su 20 che il 16 Ottobre di ogni anno Sircam cancelli tutti i file e le cartelle contenuti nell'unità C ma funziona solo sui computer che usano un formato della data Giorno/Mese/Anno come quello italiano e non Mese/Giorno/Anno come il formato americano. In aggiunta questa operazione sarà eseguita immediatamente, indipendentemente dalla data, se il file allegato al worm contiene la sequenza "FA2" senza le lettere "SC" seguenti alla sequenza.

9. Se questo provvedimento viene attivato, viene creato il file C:\Recycled\Sircam.sys e viene riempito con testo fino a che non ci sia più spazio libero sul disco. Il testo è uno di questi due:
•`[SirCam_2rp_Ein_NoC_Rma_CuiTzeO_MicH_MeX]`
oppure
• `[SirCam Version 1.0 Copyright ¬ 2000 2rP Made in / Hecho en - Cuitzeo, Michoacan Mexico]`

10. Il worm contiene un proprio motore SMTP che viene usato per la routine di invio delle E-Mail per la propagazione del worm. Sircam ottiene gli indirizzi E-Mail dei destinatari in due modi diversi:
• Cerca le cartelle che sono indicate dalle chiavi di registro `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache` e `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal` per il file che iniziato per sho*, get*, hot* e quelli con estensione htm per copiare gli indirizzi email presenti nel file C:\Windows\System\sc?1.dll dove ? è una lettera variabile a seconda della locazione: può essere Y se gli indirizzi provengono dalla prima chiave di registro e dai file che iniziano per sho, hot e get, può essere T per quelli della stessa directory ma provenienti da file con estensione htm. Per quelli provenienti dalla seconda chiave di registro la lettera variabile può essere H se sono prelevati dai file che iniziano per sho, hot e get oppure I per gli indirizzi provenienti dai file htm.
• Cerca gli indirizzi a cui spedire l'infezione nei file wab nella cartella di sistema e le sue sottocartelle e copia gli indirizzi trovati nel file scw1.dll contenuto nella cartella di sistema.

11. Cerca le cartelle a cui sono indirizzati i valori nelle chiavi di registro `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal` e `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop` per scovare file con estensione doc, xls e zip e inserire i loro nomi nel file scd.dll, nella cartella di sistema. Uno di questi file selezionati verrà preso a caso e associato al file originale eseguibile che contiene il worm e questo nuovo file nato dall'unione dei due sarà l'allegato delle E-Mail.
Il campo del mittente e il server E-Mail sono presi dal registro e se non esiste alcun account email ne verrà creato uno con dominio "prodigy.net.mx"; ad esempio se l'username dell'utente sarà mercantile allora l'indirizzo E-Mail sarà mercantile@prodigy.net.mx. Poi il worm provvede a connettersi ad un server della posta che sarà sempre scelto dal registro o sarà uno dei seguenti: prodigy.net.mx, goeke.net, enlace.net, dobleclick.com.mx. La lingua usata nell'E-Mail dipenderà dalla lingua usata sul computer del mittente infetto e varierà tra Inglese e Spagnolo; l'allegato sarà scelto a caso dalla lista dei file in scd.dll.



Istruzioni per la rimozione

Pochi giorni dopo la diffusione di quest worm i produttori di antivirus avevano già provveduto ad inserirlo nelle loro liste, nelle definizioni degli AntiVirus e a realizzare un efficiente software in grado di rimuovere l'infezione senza dover ricorrere alla procedura manuale. Potete scaricare il tool di Symantec all'indirizzo www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.removal.tool.html
• In alcuni casi, se avete messo in quarantena o cancellato i file infetti, non sarete in grado di avviare i file exe ma il software per la rimozione dovrebbe essere comunque in grado di partire.
• Se state usando Windows Me e una copia del worm viene rilevata nella cartella _Restore durante l'utlizzo del software per la rimozione, questa copia non potra essere rimossa dalla cartella perchè viene protetta da Windows.
• Se siete su un network o avete una connessione a tempo pieno ad Internet, disconnettete il computer dal netword e da Internet perchè questo worm si diffonde usando le cartelle di file in condivisione sui computer collegati a network ed è quindi consigliabile usare delle password di protezione per garantire l'accesso solo ad utenti autorizzati.

{RoSwEIL}

COME IMPOSTARE CORRETTAMENTE I DNS IN WINDOWS 2000 E NT

I TRASFERIMENTI DI ZONA DEI DNS

Una caratteristica dei server DNS può essere sfruttata per ottenere informazioni potenzialmente pericolose su un particolare network.

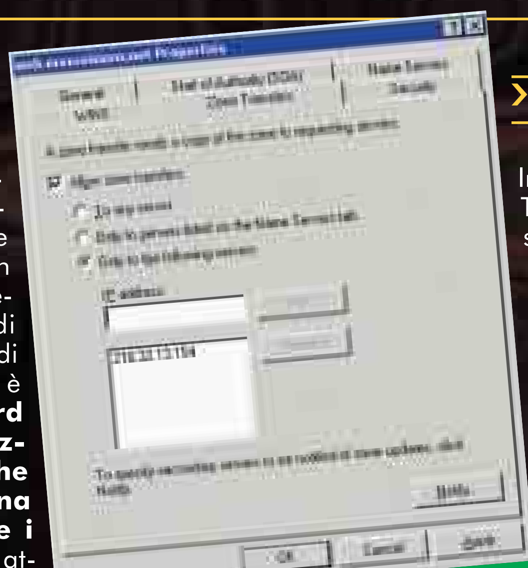
Continuiamo la nostra panoramica sull'enumerazione dei sistemi trattando gli ambiti che per questione di spazio non abbiamo introdotto nel precedente articolo. Primo di questi è il Trasferimento di Zona del DNS. Quest'ultima è **una procedura standard dei server DNS ed è utilizzata per fare in modo che i server secondari di una rete possano aggiornare i loro database di zona**, attingendo da un server DNS primario. Generalmente, quindi, un trasferimento di zona viene richiesto esclusivamente da un DNS secondario a un DNS primario. Se per esempio la nostra rete è configurata con un suo server DNS, è normale che esso richieda dei trasferimenti di zona ad un DNS di livello superiore (per esempio quello del gestore della linea dedicata). Quando si verifica un trasferimento di zona?

Quando si sta avviando un servizio DNS sul server secondario.

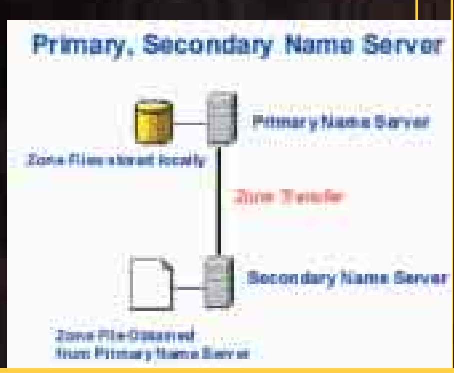
Quando il tempo di refresh del database e trascorso.

Quando sono state effettuate delle modifiche sulla Primary Zone del proprio DNS e c'è una Notify List cioè una lista di server DNS cui notificare la modifica.

Questa comunicazione viene effettuata sulla porta 53 tcp/udp e **non può essere impedita dall'amministrazione di sistema con l'inserimento di un firewall** senza provocare un malfunzionamento del servizio DNS, perciò è necessario garantirla ma **con le opportune restrizioni che vedremo**.



L'impostazione del trasferimento di zona nella MMC:



>> Come funziona

Iniziamo con alcune prove di richiesta di uno Zone Tranfer attraverso l'utility nslookup fornita in tutti i sistemi Unix-like (Linux compreso) e nei sistemi NT/2000. Se per esempio richiamiamo dalla console il comando

```
nslookup -ipsevrerdnstarget
```

dovremmo ricevere informazioni (IP e nome) sul server DNS che stiamo interrogando:

```
C:\>nslookup - 193.43.142.2
Server predefinito:
pincopallino.it
Address:  192.168.142.3

>_
```

Come potete notare, il prompt adesso è cambiato poiché siamo entrati nel programma lookup; a questo punto, per avere l'elenco di tutti i record, non dobbiamo fare altro che lanciare il comando

```
ls -d nomedominio
```

Naturalmente, la maggior parte dei server DNS dei grossi gestori sono ben configurati, perciò **è probabile che di fronte a questo comando riceviate una risposta negativa** del tipo 'Impossibile visualizzare dominio XXXXX : BAD ERROR VALUE'. Questo significa che il sistema è configurato per ricevere richieste esclusivamente da alcuni host (server DNS secondari).

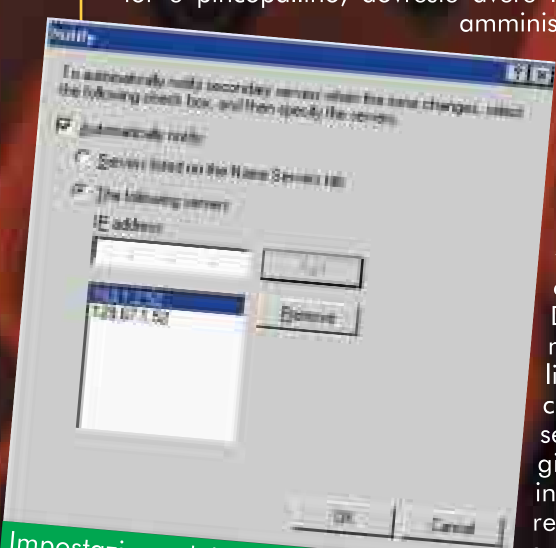
>> Una risposta rischiosa

Qualora il server non sia ben configurato il sistema potrebbe restituirvi un elenco simile a questo:

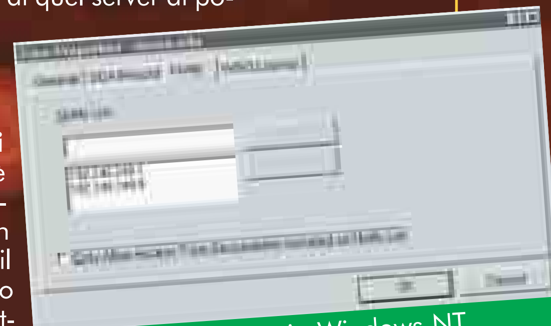
```
> ls -d pincopallino.it
[pincopallino-pdc.pincopallino.it]
 pincopallino.it.                 SOA
```

```
pincopallino-pdc.pincopallino.it
 administrator.pincopallino.it. (XX XXXX
XXX XXXXX XXXX)
 pincopallino.it.                  NS
pincopallino-pdc.tecnogen.it
 pincopallino.it.                  NS
dns1.provider.it
 pincopallino.it.                  MX      0
pincopallino-pdc.pincopallino.it
 intsederoma                        A
192.168.138.2
 intsedemilano                     A
192.168.28.1
 tg-ricerca-pdc                    A
193.43.142.2
 www                                  CNAME
pincopallino-pdc.tecnogen.it
 pincopallino.it.                  SOA
pincopallino-pdc.tecnogen.it
 administrator.pincopallino.it. (XX XXXX
XXX XXXXX XXXX)
>_
```

Vediamo qual è il significato dei vari tipi di record restituiti:
Il primo record è il SOA (Start Of Authority), record principale che ci comunica quale macchina del dominio si occupa della risoluzione dei nomi; in questo caso pincopallino-pdc. **Subito dopo abbiamo administrator.pincopallino.it**: sostituendo il punto con una '@' tra administrator e pincopallino, dovreste avere la mail del contatto amministrativo. I gruppi di x all'interno delle parentesi rappresentano dei valori numerici che indicano varie informazioni, tra cui il numero seriale che viene incrementato ogni volta che il DNS viene aggiornato e che viene utilizzato dai server secondari per sapere se ci sono degli aggiornamenti.,Oppure indicano il tempo di refresh, cioè ogni quanto tempo i server secondari si riconnettono per l'update ed altre informazioni di questo tipo che benché interessanti tralasciamo.


Impostazione della notifica automatica.

I record NS indicano i Name Server che vengono a loro volta utilizzati dal server in esame: nel nostro caso dns1.provider.it
I record MX (Mail Exchange) ci dicono dove viene processata la posta indirizzata al dominio pincopallino.it, nel nostro caso è sempre pincopallino-pdc che se ne occupa. Di record MX ve ne possono essere più d'uno, infatti, il numero che vedete nel record (nel nostro caso 0) indica l'ordine di priorità di quel server di posta: lo zero indica la priorità più alta.
I Record A servono per svolgere l'attività principale di un server DNS e cioè quella di collegare i nomi agli indirizzi IP. In questo caso abbiamo il record del server stesso (necessario per il corretto funzionamento) con in più due altri record che si riferiscono alle Intranet delle sedi di Roma e Milano dell'azienda d'esempio.


Proprietà della zona in Windows NT.

Infine il record CNAME (Canonical Name Record) serve ad attribuire ad una stessa macchina più nomi di cui quello definito con il record A è per così dire il 'primario' quelli attribuiti con CNAME i secondari.

>> Rischi e soluzioni

Come avrete notato, **le informazioni che un qualunque utente Internet avrebbe potuto ottenere dal trasferimento sono di notevole interesse**, in particolare gli IP delle intranet delle sedi distaccate dell'azienda fanno pensare alla presenza di dati particolarmente sensibili, e quindi a obiettivi di notevole interesse. È vero che informazioni di questo tipo **si potrebbero ottenere ugualmente con uno scanning della classe di ip** ma in questo caso ci troveremmo di fronte ad una macchina di cui ignoriamo la funzione all'interno dell'azienda.
Come si può evitare che questo avvenga sulla nostra rete?
In Windows 2000 è necessario richiamare la Microsoft Management Cosnole, andare in Services and Applications | DNS | [nome_server] | Forward Lookup Zones | [nome_zona] | Properties. A questo punto dovreste trovarvi di fronte la finestra di Figura 1. Di default il DNS consente il trasferimento di zona a ogni server che lo richieda; è possibile bloccare completamente questa possibilità deselezionando l'opzione 'allow zone transfers', cosa che può essere fatta soltanto se non ci sono altri server DNS nella rete che hanno bisogno di aggiornarsi dal nostro, oppure è possibile restringere le richieste di trasferimento soltanto a quelli definiti nella lista dei Name Server o specificandone gli indirizzi ip. È inoltre possibile cliccando sul tasto Notify (Figura 2) stabilire quali siano i server cui notificare eventuali cambiamenti sul nostro DNS.
In Windows NT l'operazione è leggermente diversa ma ugualmente semplice: andate sugli Administrative Tools e cliccate sul DNS Manager, a questo punto selezionate col tasto destro l'icona della Primary zone; selezionando il tab Notify vi trovate di fronte una finestra simile a quella di Figura 3. Selezionando l'opzione 'Only Allow Access From Secondaries Included on Notify List', è possibile limitare le richieste di trasferimenti di zona ad un elenco di server da voi redatto.

Roberto "dec0der" Enea

I RISCHI DEI FILE DESKTOP DB E DESTOP DF DI MAC OS

Caccia ai Desktop file

...cioè a quei piccoli file invisibili che pochi conoscono, ma che possono rappresentare una minaccia per la privacy.





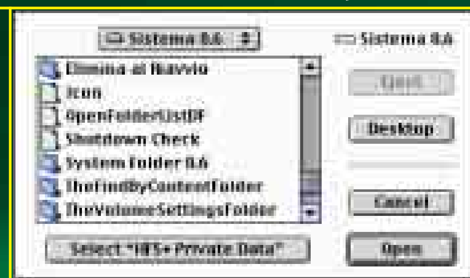
Come altri sistemi operativi, anche **l'OS del Macintosh contiene sui suoi supporti di archiviazione una serie di file e risorse nascosti all'utente** finale ma indispensabili al corretto funzionamento della macchina.
A guardare con attenzione, il Mac OS "classico", e cioè tutti le versioni precedenti ad X (fino al 9.2, l'ultima), è disseminato di cartelle e file invisibili, in particolare a livello primario dell'hard disk (l'equivalente della 'root' in altri sistemi) in cui è contenuto l'OS. Usando tool come il vecchio Norton Disk Editor o anche qualsiasi programma che abbia una funzione di "Apri" un po' più smaliziata, è possibile **esaminare con maggiore attenzione la cartella in questione**. Il risultato sarà un'interessante lista di file, simile a questa:

```
HFS+ Private Data
Cleanup At Startup
Desktop Folder
Elimina al Riavvio
System Folder
Temporary Items
TheFindByContentFolder
TheVolumeSettingsFolder
Trash
Desktop DB
Desktop DF
Desktop PN
Desktop
OpenFolderListDF
Icon
Shutdown Check
DesktopPrinters DB
AppleShare PDS
```

L'unico oggetto normalmente visibile nel Finder è "System Folder", meglio nota come "Cartella Sistema" nelle versioni italiane del MacOS. L'altra dozzina di elementi assolve a funzioni quali eliminare file temporanei dopo le installazioni ("Cleanup At Startup" e "Elimina al Riavvio"), contenere file da mostrare sulla scrivania ("Desktop Folder", che equivale grosso modo al noto C:\WINDOWS\Desktop), ricordarsi delle icone personalizzate ("Icon") o delle cartelle aperte e della loro posizione ("OpenFolderListDF").







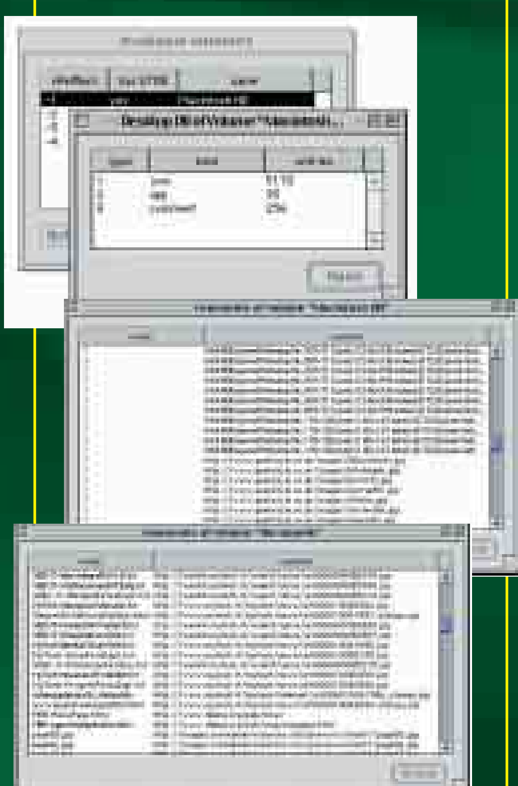
>> Uno sguardo ai file

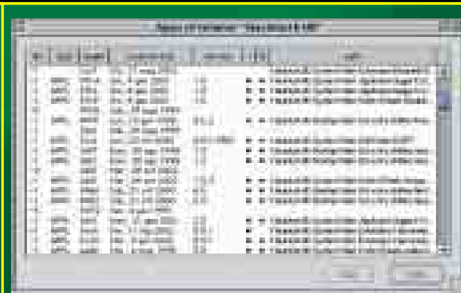
Tra questi ci sono alcuni file il cui contenuto riserva delle sorprese all'utente: Desktop, Desktop DB e Desktop DF. Questi file sono sempre presenti e sono sostanzialmente dei **database che servono tenere traccia di tutti i documenti e le applicazioni sull'hard disk**: grazie a loro il Macintosh mostra correttamente le icone e soprattutto si ricorda che facendo doppio clic su un documento deve lanciare il programma ad esso associato. Le sigle "DB" e "DF" stanno per "Desktop Bundle" e "Desktop Files" (sì, i nomi sono ricorsivi) mentre "Desktop" assolve alla stessa funzione ma era usato sui sistemi molto vecchi, prima della versione 7 ed è tenuto per compatibilità con il passato e per i dischi di dimensioni molto piccole (floppy disk per esempio).
Gli utenti Macintosh sanno che, come manutenzione, **è buona norma di tanto in tanto "ricostruire il desktop", cioè riaggiornare il database dei file**. La procedura può essere fatta tramite utility ad hoc (Norton, Tech Tool) o semplicemente riavviando la macchina tenendo premuti i tasti Comando (Mela) e Opzione (Alt) fino alla comparsa della scrivania e dando OK alla richiesta che compare. Un file di desktop troppo grande e vecchio

può rallentare le prestazioni, aprire i documenti con i programmi sbagliati (o non aprirli affatto) e mostrare icone "generiche" per i file.

>> Un rischio per la privacy

Quello che però non tutti sanno è che modificare o aggiornare i desktop file può essere fatto anche per questioni di privacy. Il Desktop DB contiene al suo interno una serie di dati, tra cui **i nomi dei file, le loro posizioni sul disco fisso, i commenti inseriti, gli url dei siti visitati e dei file scaricati** (e generalmente "poggiati" sulla scrivania). Insomma **una miniera di informazioni sensibili e riservate che potrebbe essere usata anche contro di noi**.
Per guardare all'interno del Desktop DB e verificare l'effettivo contenuto si può usare l'utility Desktop DB Diver (www.tempel.org/ftp/pub/Mac/DesktopDBDiver.sit) di Thomas Tempel. Basta lanciarla, selezionare il volume o la partizione che ci interessa (nel nostro caso quella standard, "Macintosh HD") e scegliere la voce "app" o "comment". C'è effettivamente da preoccuparsi e **la situazione si fa drammatica**

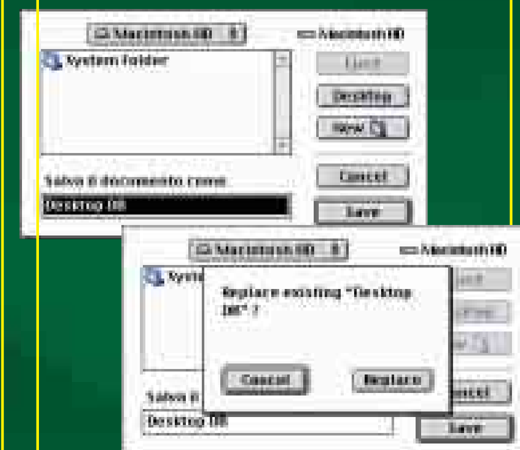




quando si scambiano dati con altri. Masterizzando CD in formato ISO9660 (il formato standard su Windows ed altri sistemi) il Macintosh non solo include i file Desktop DB e DF del disco da cui si prendono i file, ma li può rendere visibili (basta un semplice editor di testi come Notepad), **permettendo a chiunque di ficcanasare tra le nostre operazioni in rete e non**.

>> Tuteliamoci!

Come correre al riparo? In vari modi: anzitutto dopo le proteste di migliaia di utenti **le ultime versioni del più diffuso programma di masterizzazione per Mac, Toast, permettono di eliminare, o meglio di includere file Desktop DB e DF "vuoti" al momento di creare il CD**. Una buona cosa, quindi sarebbe aggiornare Toast all'ultima versione disponibile (www.roxio.com/en/ support/roxio_support/toast/toast_software_updatesv5.jhtml).
Un altro modo di evitare il problema può essere quello di **masterizzare i dati da una partizione (vera o virtuale) o immagine disco, create ex novo**, i cui desktop files sono "vergini". Questo si può fare da Toast, anche nelle vecchie versioni, oppure con l'utility di Apple "Disk Copy", acclusa in ogni MacOS.
Ci sono inoltre delle utility che possono correre in nostro aiuto. Una è "TrashDesktop" (www.opus.plugin.ch/freeware), che rende tutti e tre i file "Desktop DB", "Desktop DF" e "Desktop" visibili e li sposta nel cestino. Basta riavviare e poi vuotare il cestino.
Un'altro aiuto ci viene da "Total Desktop Rebuild" (http://persoweb.francenet.fr/~alm/binhex/total-desktop-rebuild-11.hqx) che "forza" una ricostruzione totale dei file "desktop".
Infine, **per chi magari non si fida o vuole ricorrere a metodi più diretti e artigianali è possibile forzare con un trucco la creazione di nuovi indici**. Per farlo è sufficiente un qualsiasi editor di testi.
La prima operazione è chiudere tutti i programmi aperti (eccetto il Finder, ovviamente) per poi lanciare l'editor, aprire un nuovo documento e, anche vuoto, salvarlo con il nome "Desktop DB" (senza le virgolette) dentro il livello primario del disco fisso.



Nella finestra di dialogo il sistema chiederà se si vuole rimpiazzare un file preesistente. Ovviamente la risposta è sì. Lo stesso si può fare per "Desktop DF". Chiudiamo il programma, apriamo la cartella dell'hard disk e cestiniamo i due file ora visibili. A questo punto basterà riavviare e poi svuotare il cestino per avere... la coscienza pulita.

Nicola D'Agostino
dagostino@nezmar.com

APPROFONDIMENTI

Desktop DB Diver
www.tempel.org/macdev
Desktop Manager Q&As
http://developer.apple.com/technotes/tb/tb_520.html
TB 535 - Finder Q&As
http://developer.apple.com/technotes/tb/tb_520.html
OPS 03 - Desktop Using Icons from Old Versions of Applications
http://developer.apple.com/qa/ops/ops03.html